RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: HTA-M03

QuickShell: Sharing is Caring About an RCE Attack Chain on Quick Share

Or Yair

Security Research Team Lead
SafeBreach
https://www.linkedin.com/in/or-yair/

Or Yair

- Security Research Team Lead at SafeBreach
- 7+ years in Security Research
- Past research in Linux, embedded, Android
- 4 years Windows research

Shmuel Cohen - Contributor

- 6+ years in Security Industry
- Past APT Malware Researcher
- 4+ years Windows research

Agenda

– Пc v ЯПЎψ { ПҚ,SS

t St Д Ҷt ζh кSSkTSл

CЯЦЦTvZ

wSJTSK,SЎП! ТЪЗSt Қ,ЎП { ПТВ • ЯҚvSSK,nTζДc 5 JTЎt кSSc

w/ 9 / ПҚ,Tv

ƒK,γSK,л Қ,cЛЬ

DTД Яn v !

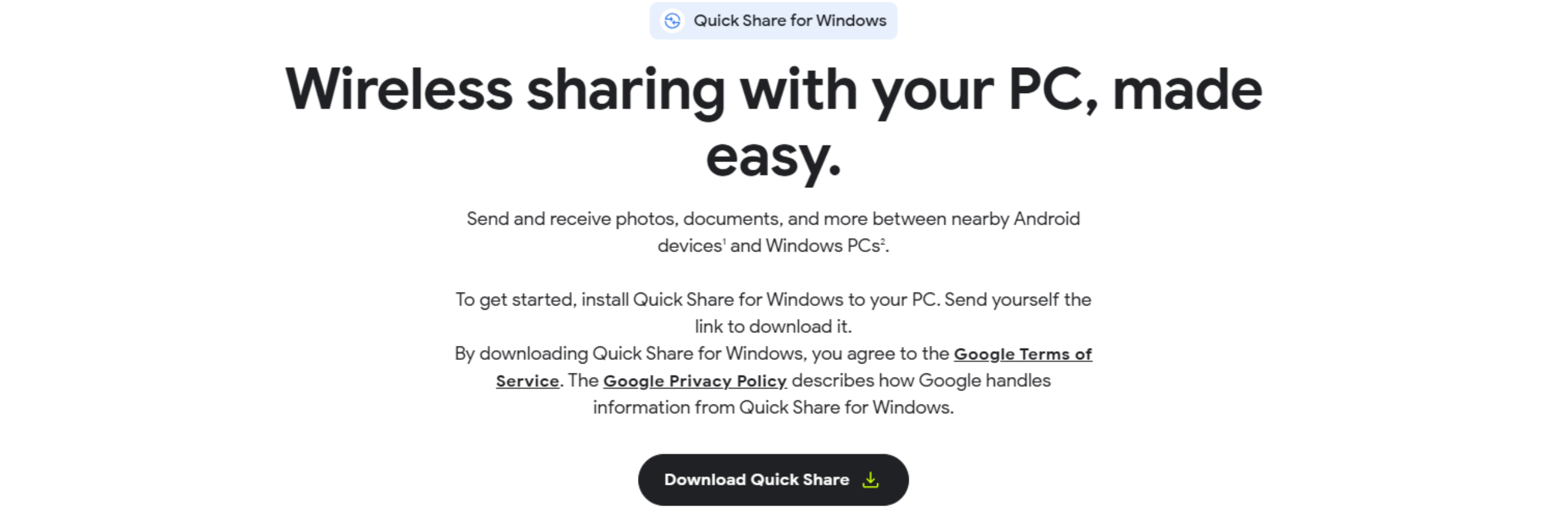
What is Quick Share?

Quick Share

2:42
Quick Share
You'll share as
Pixel 8 Pro
Send to your devices
Pixel 8
Sending...
Send to nearby devices
Looking for nearby devices...
2:42
Tue, Jan 23
Receiving...
From Pixel 8 Pro
1 image
Cancel

Why Quick Share?

Quick Share Windows Version


Quick Share for Windows
Wireless sharing with your PC, made easy.
Send and receive photos, documents, and more between nearby Android devices[1] and Windows PCs[2].
To get started, install Quick Share for Windows to your PC. Send yourself the link to download it.
By downloading Quick Share for Windows, you agree to the Google Terms of Service. The Google Privacy Policy describes how Google handles information from Quick Share for Windows.
Download Quick Share

Quick Share Pre-installation

ANDROID

What we announced at CES 2024

Jan 09, 2024 · 6 min read

Quick Share Communication Methods

• ĶŞŠţ ЯЛЬЙţ µ µ ЯѵТЎĶЙţ ѵ
µ ŞДПţ ŘЛЬ

ЛДЙµ Ş ņc Dţ ţ ZĢŞ
ţ ѵ – ŤѵŘţ л ЛЬ

Previous Research

- 2019 by Daniele Antonioli, Nils Ole Tippenhauer, Kasper Rasmussen:
- “Nearby Threats: Reversing, Analyzing, and Attacking Google’s ‘Nearby Connections’ on Android”
  - About Nearby Connections API
  - Only Android
  - No CVEs

Nearby & Chromium Open-Source Repos

Contain part of the code for Quick Share for Windows

google / **nearby** Public

🐿️ A collection of projects focused on connectivity that enable building cross-device experiences.

developers.google.com/nearby

Apache-2.0 license

696 stars 151 forks Branches Tags

chromium / **chromium** Public

The official GitHub mirror of the Chromium source

chromium.googlesource.com/chromium/src/

BSD-3-Clause, BSD-3-Clause licenses found

18.3k stars 6.8k forks Branches Tags

Why Quick Share

- bŞл – TvŘtлЛЬ TЂЂ bŞл ! TЂЂbŞл кЯЋvЛЬ
- – TvŘtлЛЬ,КЂЂлTЋ,ŋŞTЂSS□TvЛД,КЋ,SŘ
- •Ķ,SttЯЛЬŇtμμЯvTŇ,ЙtvμŞДПtŘЛЬ□ •Ķ,SttЯЛЬ,УĶ,ŇўкŞŇД,SЪ
- Dttz,Ş□ЛЬźSЭД– TvŘtлЛЬ,КЂЂД,ЯЛЎŞДПŞЛЎŞ!tЦЬ
- {τμŞtŮДПŞŇtŘŞTЛtTЂŞv□ЛЬЯЭŇŞ
- bτ/•9ЛЬ

Research Goal

First RCE in Quick Share

Protocol Investigation

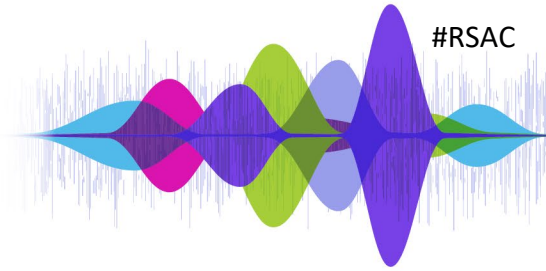
Investigating The “nearby” repo

Finding the communication functions – Send & Recv:

```
ExceptionOr<ByteArray> BaseEndpointChannel::Read(PacketMetaData& packet_meta_data)
```

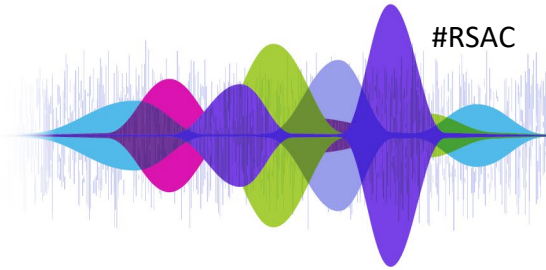
```
Exception BaseEndpointChannel::Write(const ByteArray& data,
                                     PacketMetaData& packet_meta_data)
```

Protobuf and Offline Frames




```
OfflineFrame frame;
frame.ParseFromString(std::string(bytes))
```

Protobuf and Offline Frames



offline_wire_formats.proto

```
message OfflineFrame {
  enum Version {
    UNKNOWN_VERSION = 0;
    V1 = 1;
  }
  optional Version version = 1;

  // Right now there's only 1 version, but if there are more, exactly one of
  // the following fields will be set.
  optional V1Frame v1 = 2;
}
```

v ЯПЎ{ vТ□ □ Ъfтτζ

l τγТvZv ЯПЎ{ ПҚSSД ЛъТ□ ЛЭvД
ҚvŘSSЎSkSŘhATvSCSKu SЛъv
– TvŘtлЛЬ

```
initiator_to_responder:
v1:
  payloadTransfer:
    packetType: DATA
    payloadChunk:
      body:
        v1:
          introduction:
            fileMetadata:
            - id: '585290039179534374'
              mimeType: image/png
              name: TFMyMDI0MDYxMzEzMzM1Ni5wbmc=
              payloadId: '-8969229381597391197'
              size: '622679'
              type: IMAGE
            type: INTRODUCTION
          version: V1
      flags: 0
      index: 0
      offset: '0'
    payloadHeader:
      id: '-57785711429587421 93'
      isSensitive: false
      totalSize: '85'
      type: BYTES
  type: PAYLOAD_TRANSFER
version: V1
```

Protocol Overview

bŞKŞ¸Sş¸c/τννŞŇŸτνЛЬtL

bŞKŞ¸Sş¸c/τννŞŇŸτνЛЬtL

vЯПŇγ{ПК¸Ş¸Sş¸Lμ Т§Ş¸Ş¸μ ŞνДЦЙτν

Nearby Connections API

Discover and establish direct communication channels with other devices without having to be connected to the Internet. Enables seamless nearby interactions such as multiplayer gaming, realtime collaboration, forming a group, broadcasting a resource, or sharing content.

The Nearby Connections API is available for Android and iOS, and enables communication between the two platforms.

SafeBreach

Nearby Connections API

t S: Д ņ ЯŮ. ĶЛЂŠŘ

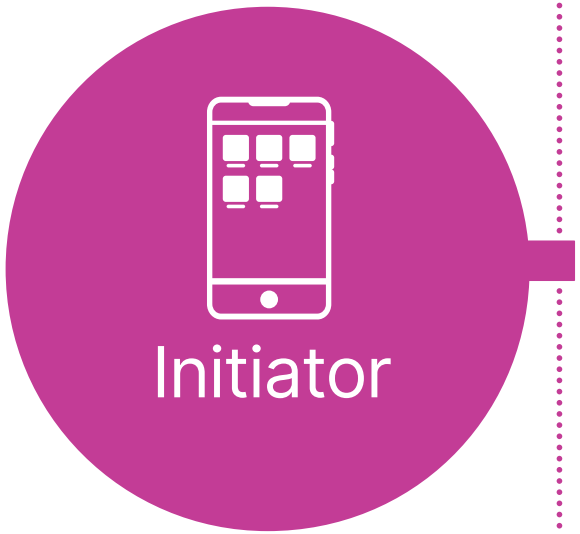
protobuf
Protocol Buffers

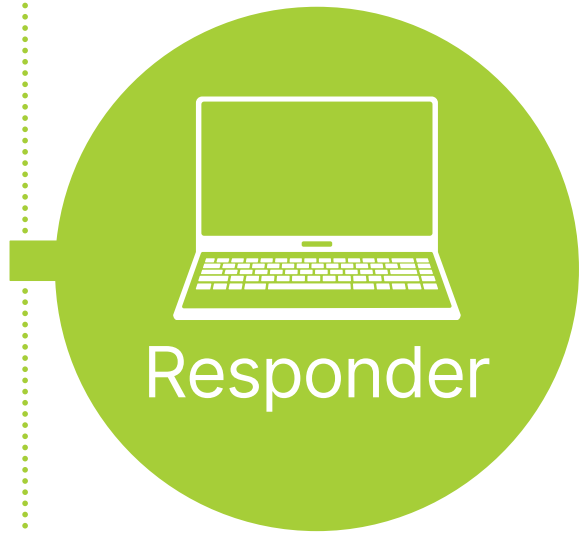
9vŇBcTЭИtv □Dττ ZÇŞJЛЂ‡γŞc□

! ŘkŞSЎИЂşu ŞvДņĶЛЂŠŘτv{ŞSkTŇŞl5

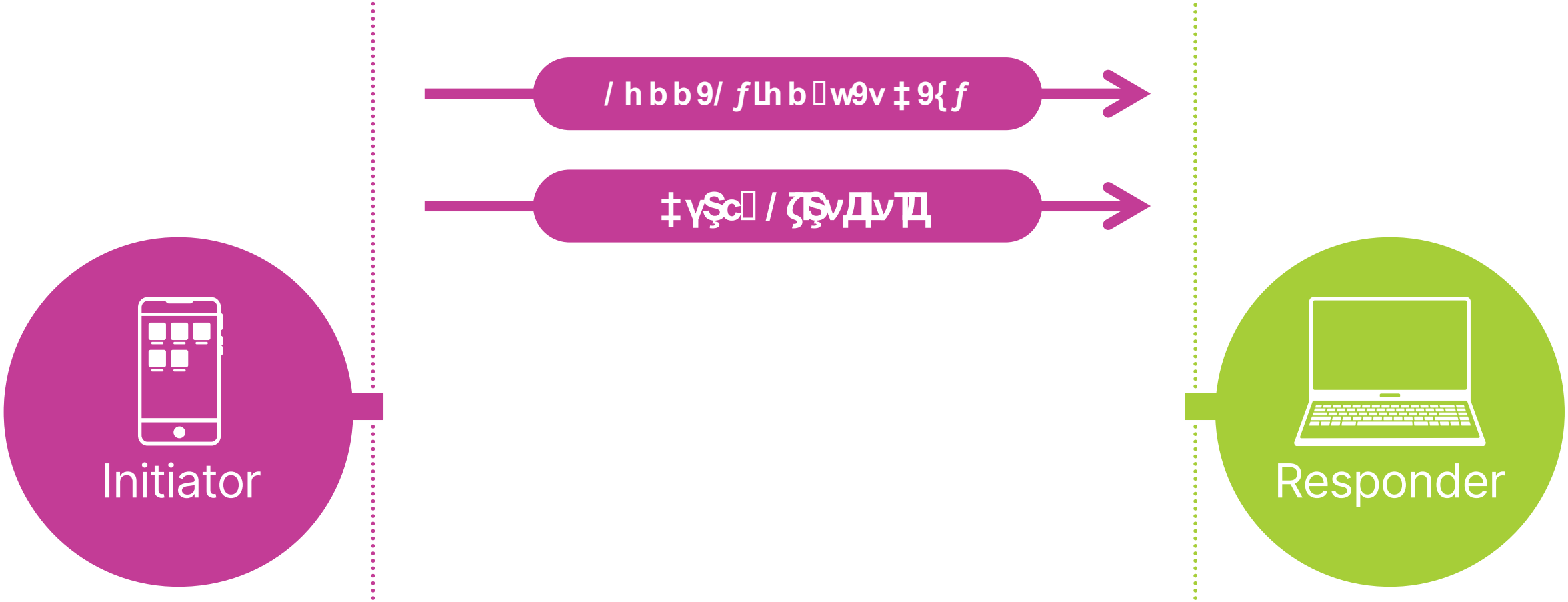
a ЯЙЛЂÇŞ/ τvvŞŇЎtvЛЪ{ДЂ,ЛЂŞZTŞЛЪ
- t □t □{ДĶS□/ ÇЯЛДЂSS

Quick Share Protocol Overview



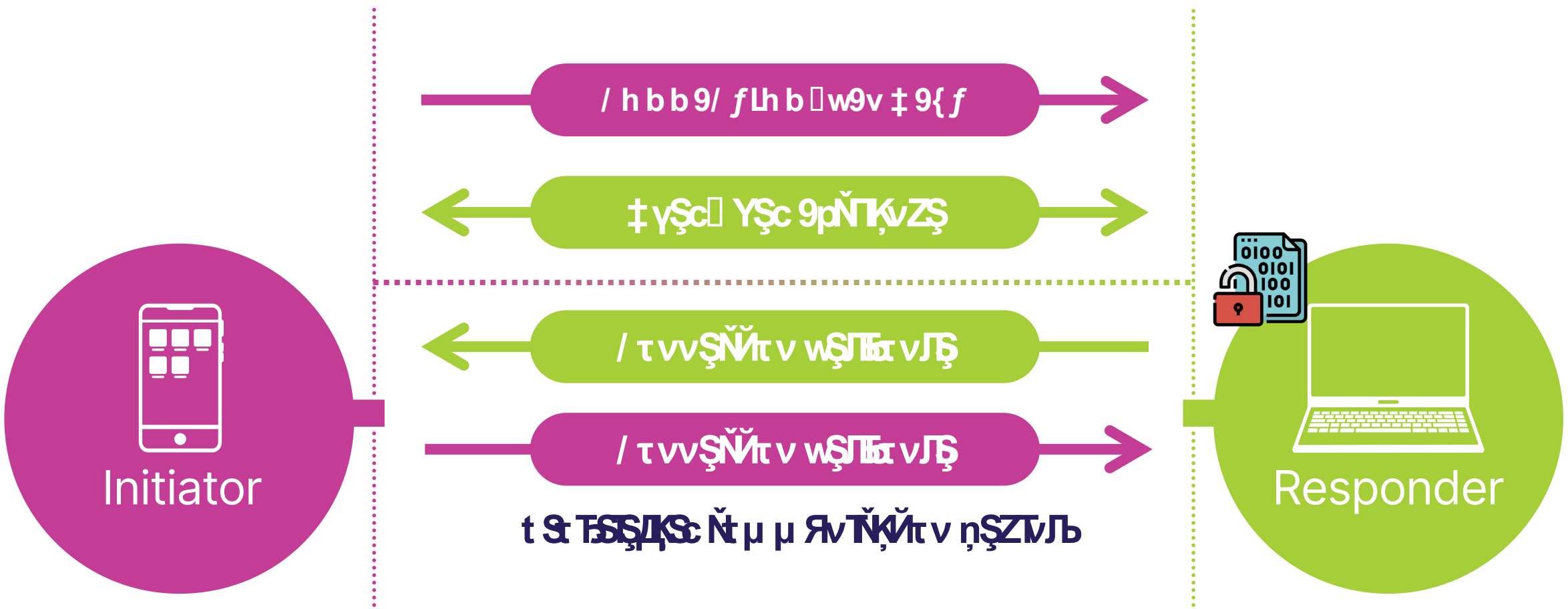


Quick Share Protocol Overview



Quick Share Protocol Overview

Quick Share Protocol Overview



Packet Types

```
enum FrameType {
  UNKNOWN_FRAME_TYPE = 0;
  CONNECTION_REQUEST = 1;
  CONNECTION_RESPONSE = 2;
  PAYLOAD_TRANSFER = 3;
  BANDWIDTH_UPGRADE_NEGOTIATION = 4;
  KEEP_ALIVE = 5;
  DISCONNECTION = 6;
  PAIRED_KEY_ENCRYPTION = 7;
  AUTHENTICATION_MESSAGE = 8;
  AUTHENTICATION_RESULT = 9;
  AUTO_RESUME = 10;
  AUTO_RECONNECT = 11;
  BANDWIDTH_UPGRADE_RETRY = 12;
}
```

Packet Types

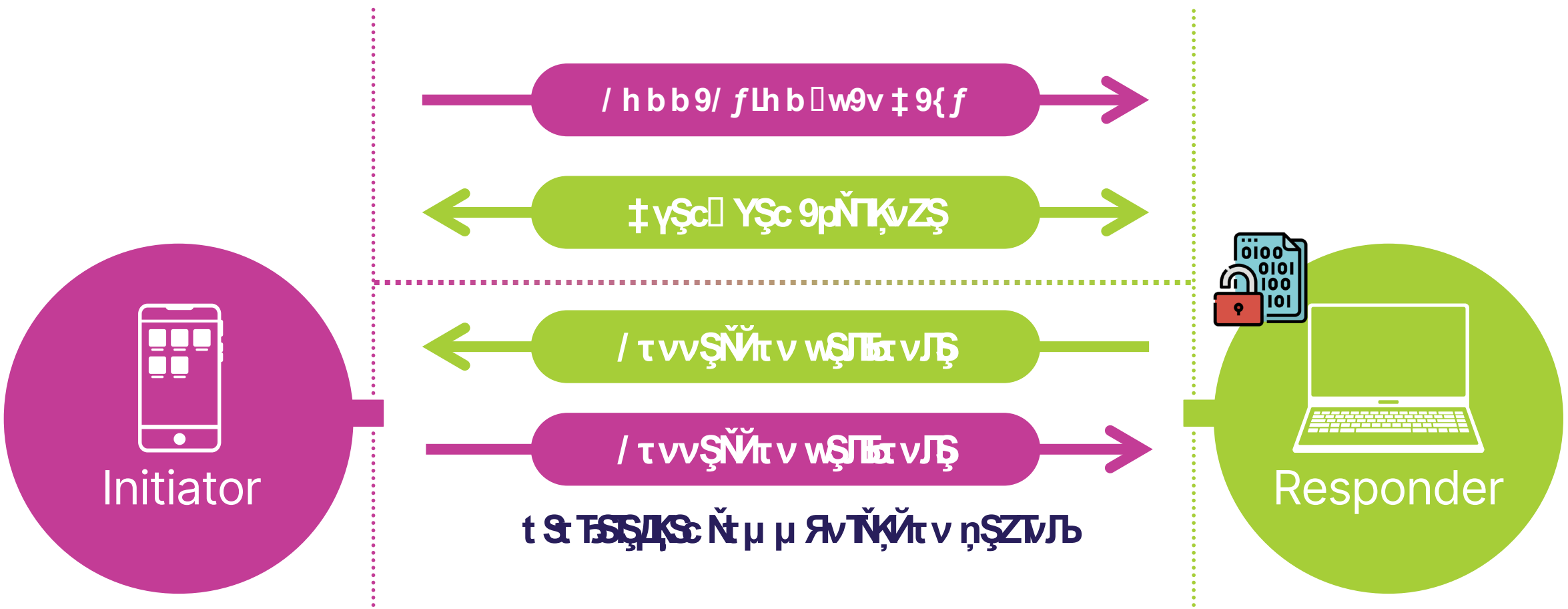
```
enum FrameType {
  UNKNOWN_FRAME_TYPE = 0;
  CONNECTION_REQUEST = 1;
  CONNECTION_RESPONSE = 2;
  PAYLOAD_TRANSFER = 3;
  BANDWIDTH_UPGRADE_NEGOTIATION = 4;
  KEEP_ALIVE = 5;
  DISCONNECTION = 6;
  PAIRED_KEY_ENCRYPTION = 7;
  AUTHENTICATION_MESSAGE = 8;
  AUTHENTICATION_RESULT = 9;
  AUTO_RESUME = 10;
  AUTO_RECONNECT = 11;
  BANDWIDTH_UPGRADE_RETRY = 12;
}
```

Packet Types

```
enum FrameType {
  UNKNOWN_FRAME_TYPE = 0;
  CONNECTION_REQUEST = 1;
  CONNECTION_RESPONSE = 2;
  PAYLOAD_TRANSFER = 3;
  BANDWIDTH_UPGRADE_NEGOTIATION = 4;
  KEEP_ALIVE = 5;
  DISCONNECTION = 6;
  PAIRED_KEY_ENCRYPTION = 7;
  AUTHENTICATION_MESSAGE = 8;
  AUTHENTICATION_RESULT = 9;
  AUTO_RESUME = 10;
  AUTO_RECONNECT = 11;
  BANDWIDTH_UPGRADE_RETRY = 12;
}
```

Quick Share Implementation

Recap



Payload Transfer

Enforces “Contacts” and “Your Devices” modes

Quick Share Implementation

Custom protobuf data in
Payload Transfer OfflineFrame

```
v1:
  payloadTransfer:
    packetType: DATA
    payloadChunk:
      body: CAESYggBEl4KWgoIYmFzZS5hcGs
      flags: 0
      index: 0
      offset: '0'
    payloadHeader:
      id: '-5454771653010976901'
      isSensitive: false
      totalSize: '102'
      type: BYTES
  type: PAYLOAD_TRANSFER
version: V1
```

```
v1:
  payloadTransfer:
    packetType: DATA
    payloadChunk:
      body:
        v1:
          pairedKeyEncryption:
            secretIdHash: palHIL+r
            signedData: MEUCIQC24J1oLakk1ypg7
          type: PAIRED_KEY_ENCRYPTION
        version: V1
      flags: 0
      index: 0
      offset: '0'
    payloadHeader:
      id: '-5454771653010976901'
      isSensitive: false
      totalSize: '102'
      type: BYTES
  type: PAYLOAD_TRANSFER
version: V1
```

Payload Transfer

Enforces “Contacts” and “Your Devices” modes

Payload Transfer

Lb ƒ wh 5 ‡ / ƒ Lh b ! / / 9t ƒ

After paired Key Encryption:

Payload Transfer

Lb ƒwh 5‡/ ƒLh b !//9t ƒ

After paired Key Encryption:

Payload Transfer

Lb ƒ wh 5 ‡ / ƒ Lh b ! / / 9t ƒ

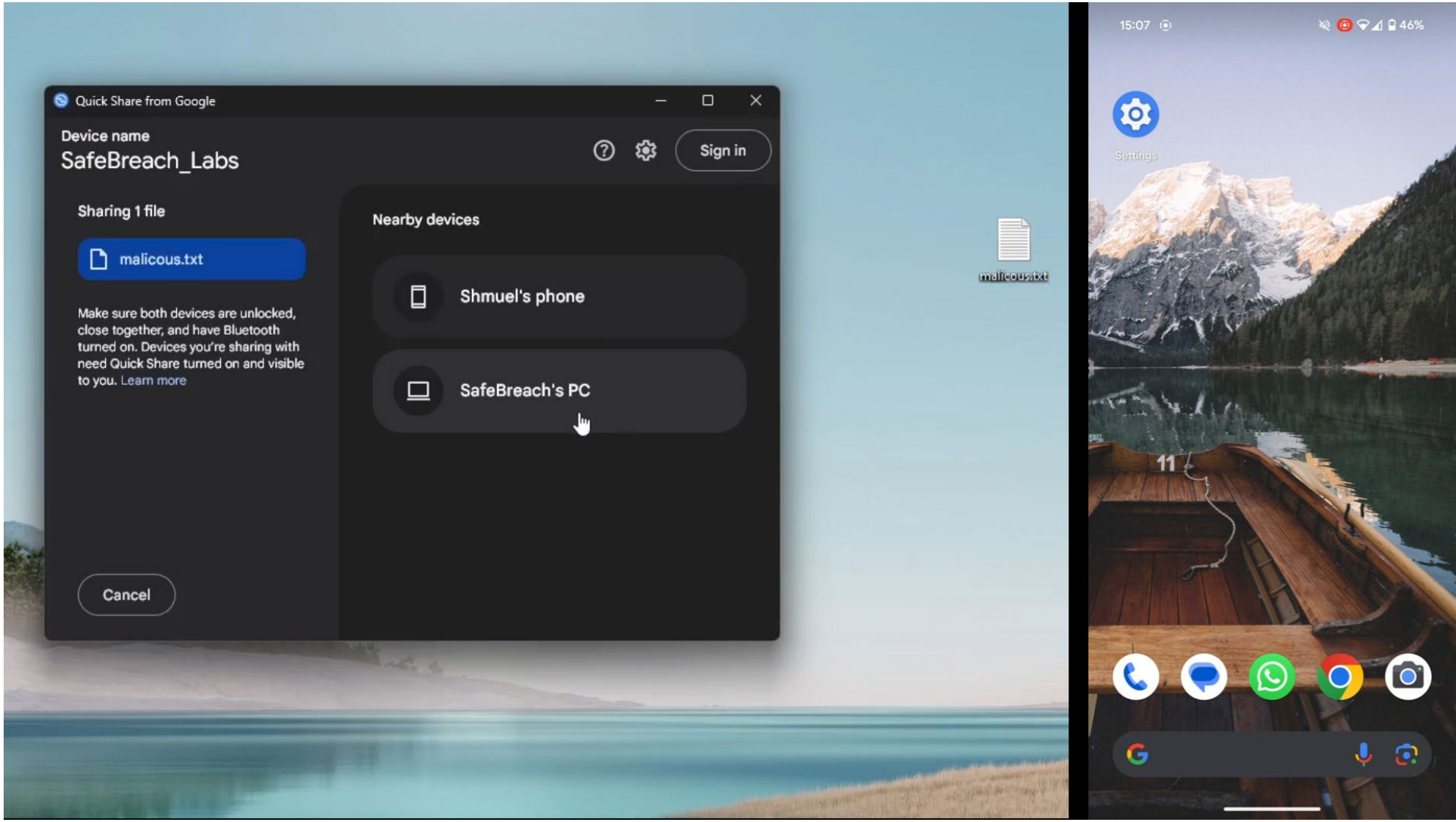
After paired Key Encryption:

Payload Transfer

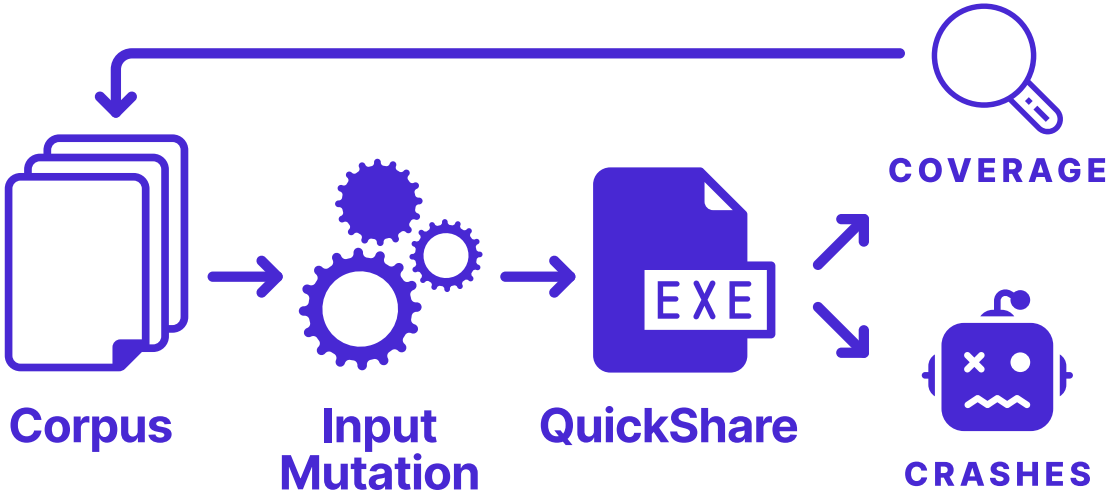
Lb ƒ wh 5 ‡ / ƒ Lh b ! / / 9t ƒ

After paired Key Encryption:

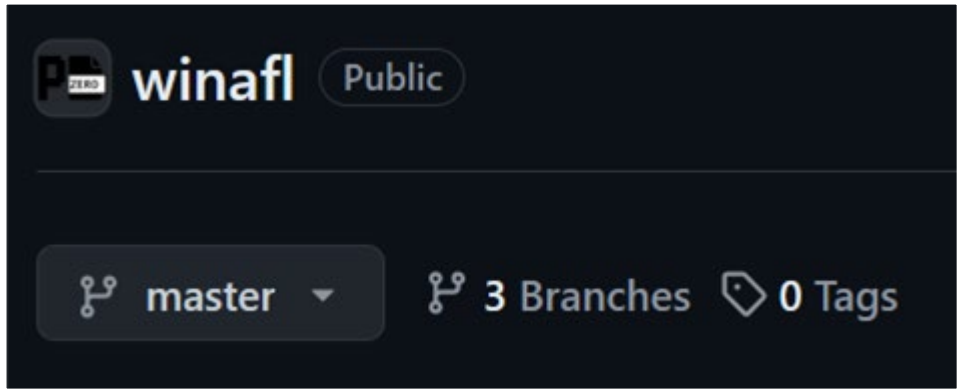
Payload Transfer



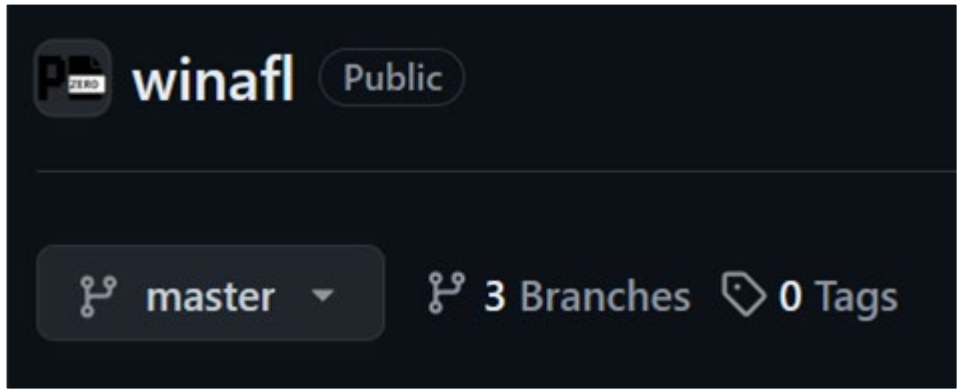
Fuzzing Quick Share



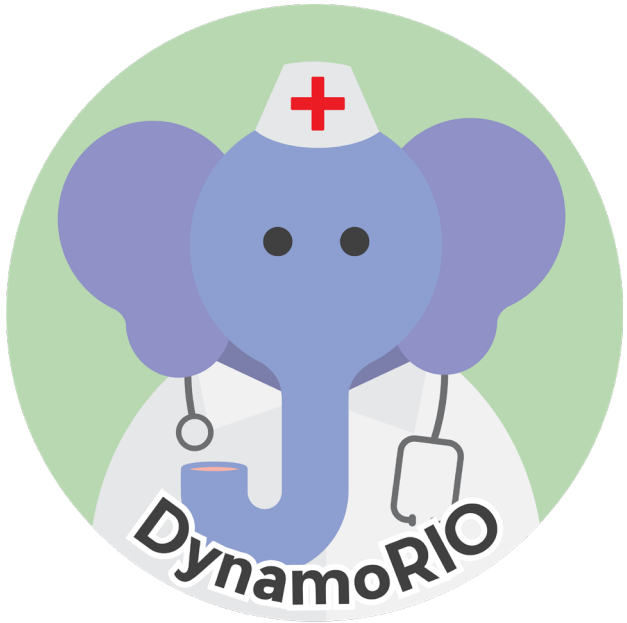
Fuzzing Infrastructure



Fuzzing Infrastructure



+



Fuzzing Infrastructure

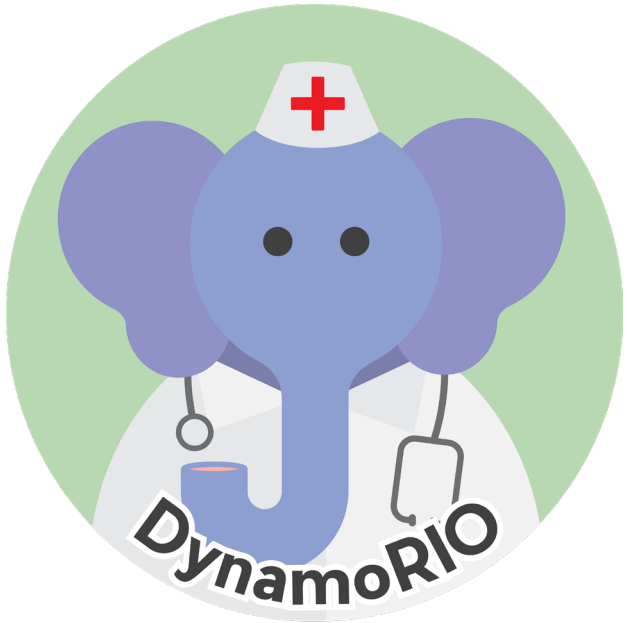
winafl Public

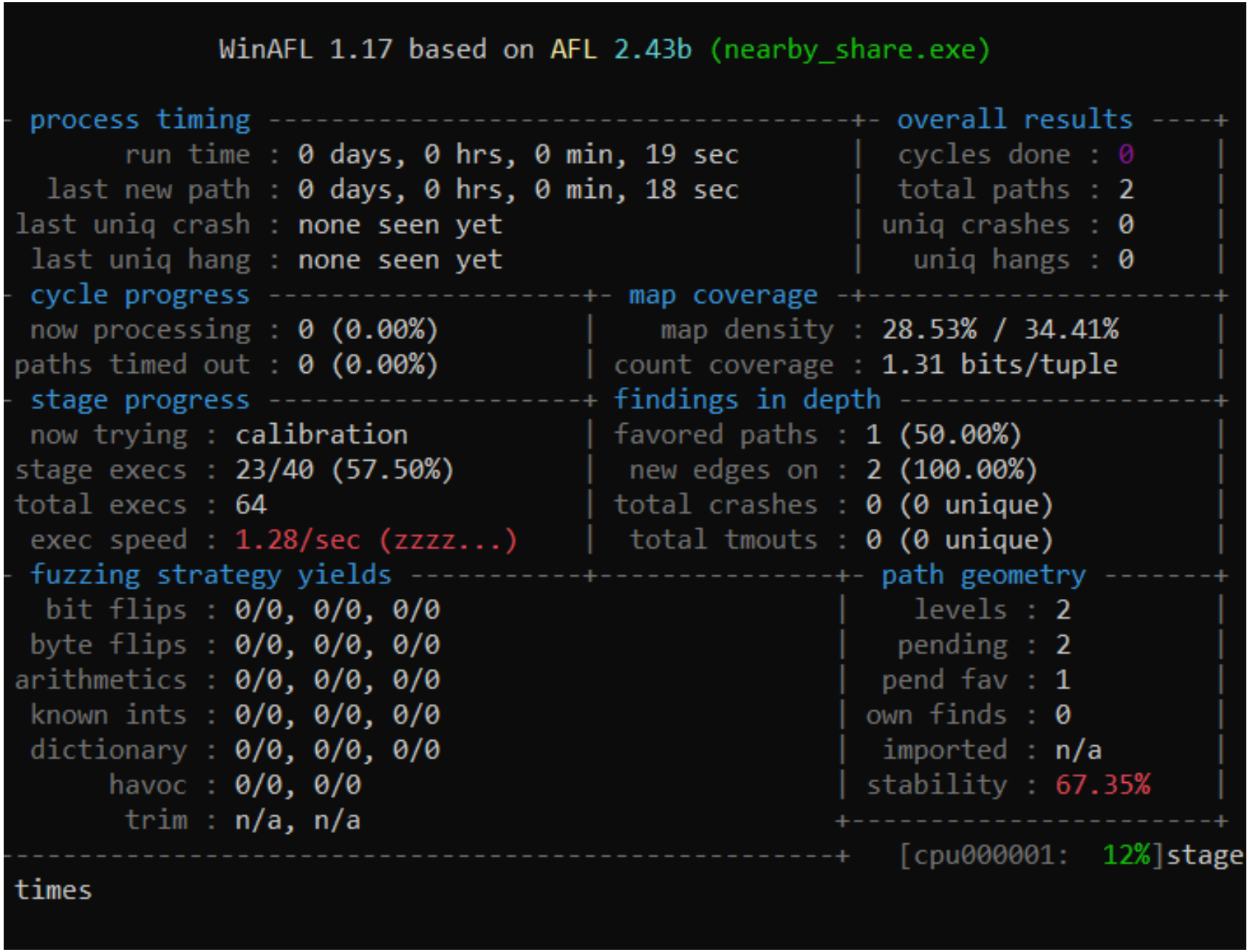
master 3 Branches 0 Tags

libprotobuf-mutator Public

master 1 Branch 4 Tags

+

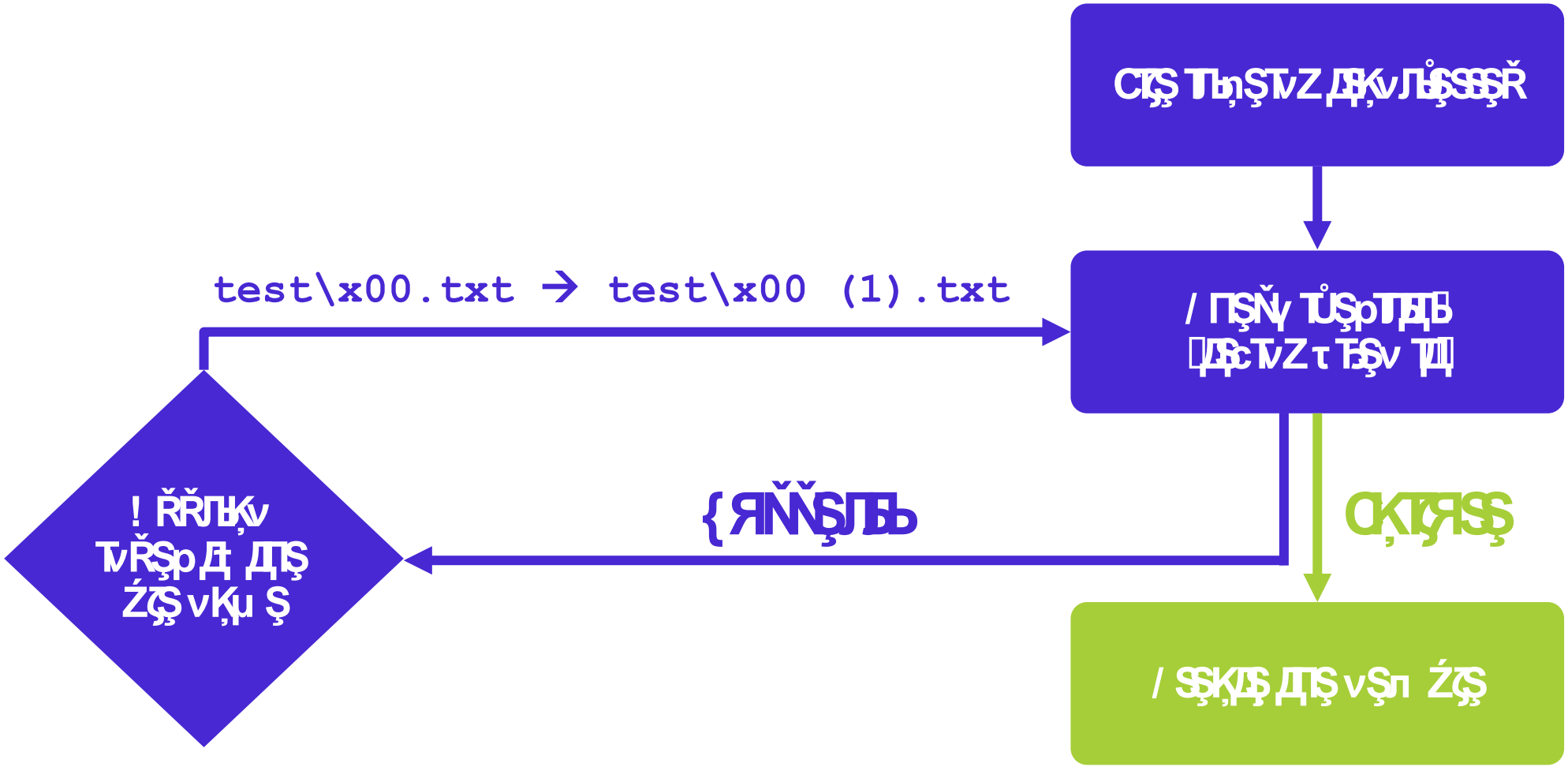



WinAFL 1.17 based on AFL 2.43b (nearby_share.exe)
process timing
run time : 0 days, 0 hrs, 0 min, 19 sec
last new path : 0 days, 0 hrs, 0 min, 18 sec
last uniq crash : none seen yet
last uniq hang : none seen yet
overall results
cycles done : 0
total paths : 2
uniq crashes : 0
uniq hangs : 0
cycle progress
now processing : 0 (0.00%)
paths timed out : 0 (0.00%)
map coverage
map density : 28.53% / 34.41%
count coverage : 1.31 bits/tuple
stage progress
now trying : calibration
stage execs : 23/40 (57.50%)
total execs : 64
exec speed : 1.28/sec (zzzz...)
findings in depth
favored paths : 1 (50.00%)
new edges on : 2 (100.00%)
total crashes : 0 (0 unique)
total tmouts : 0 (0 unique)
fuzzing strategy yields
bit flips : 0/0, 0/0, 0/0
byte flips : 0/0, 0/0, 0/0
arithmetics : 0/0, 0/0, 0/0
known ints : 0/0, 0/0, 0/0
dictionary : 0/0, 0/0, 0/0
havoc : 0/0, 0/0
trim : n/a, n/a
path geometry
levels : 2
pending : 2
pend fav : 1
own finds : 0
imported : n/a
stability : 67.35%
[cpu000001: 12%]
stage times

Reproducible Crashes

- νtν ŞpFƵtTĮĶņÇŞ5τ{ кЯĞvŞSĶņTÇЙŞЛ
- lvκĶÇŘ‡ƒC Ňtv ЙvЯĶЙtv ņcДŞ
- 9μ TĮĮc 9vŘFtTvДĮ5
- tĶcÇtĶŘl5 ЛŞĮДĮ
- CĶЛĮ Ňtvv ŞŇЙtvЛ
  - ЛĶμ Ş νtvŇŞ Tv / τvvŞŇЙtv wŞЄЯŞЛĮ
  - ‡bYbh– b• 9w{lhb ЛŞĮTv / τvvŞŇЙtv wŞЛƁtvЛŞ

Reproducible Timeout

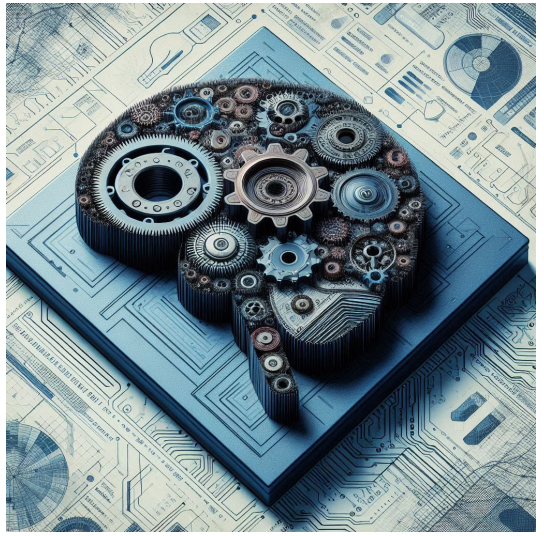


Time For Reflection

CЯЦЦ§SSTЛЫЯvvTvZ□Л§л ņЯДпtSγЛВ

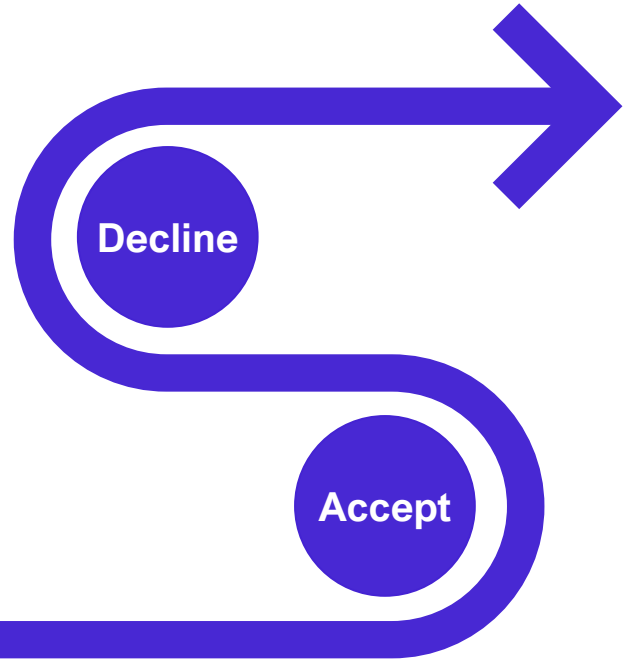
{τμ ŞЯvŞpГ§τ ТДКņ,ÇŞ ŹvŘTvZЛЬ

a τκTvZτv Д ЛЗK,SŇПЏtSζτZTŇ
кЯζvŞSЗK,nTζЇЙŞЛВTvЛДЗK,ŘtŮŇSŞK,ЙvZ
ДТŞ ГЗŞSЗŞŇДЏЯЦЦ§SS



Logic Vulnerabilities

File Acceptance Bypass



Payload Transfer

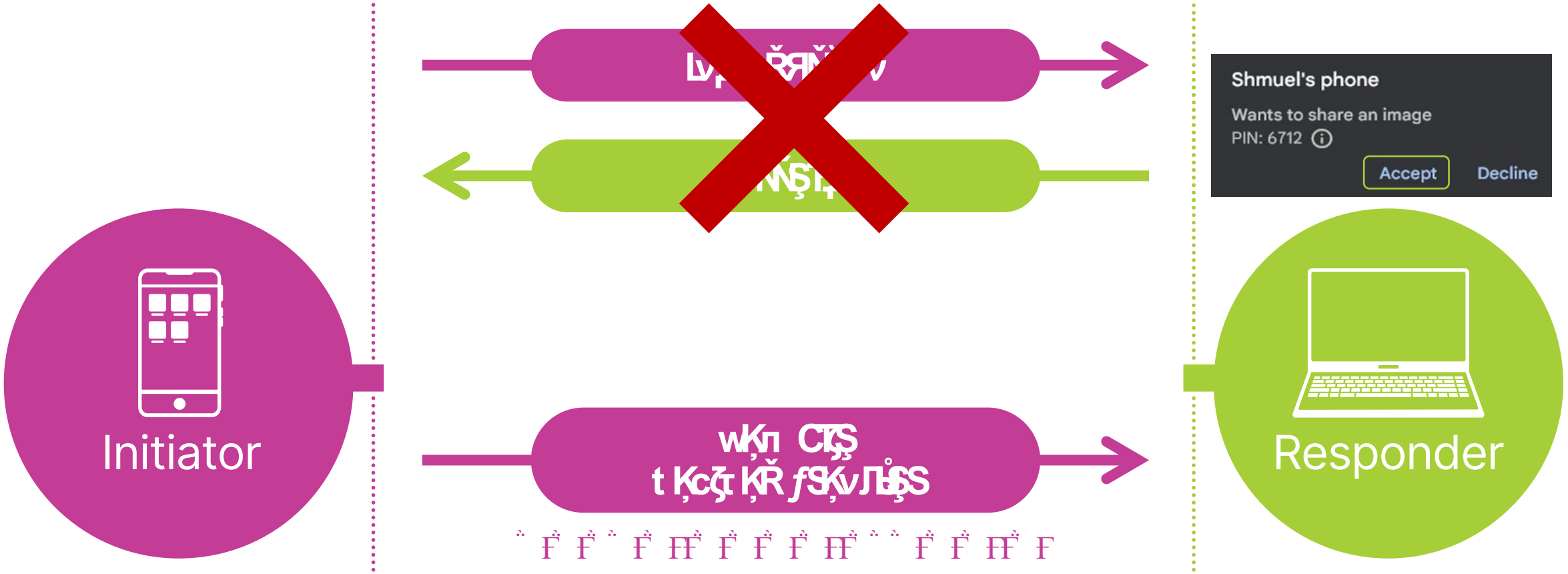
Lb ƒ wh 5 ‡ / ƒ Lh b ! / / 9t ƒ

! BŞSTĮKTSŞŘ YŞc 9v ŇSc TĮЎt v

Payload Transfer

Lb ƒ wh 5 ‡ / ƒ Lh b ! / / 9t ƒ

! BŞSTĮKTSŞŘ YŞc 9vŇBcTĮЙt v



File Transfer Acceptance Bypass

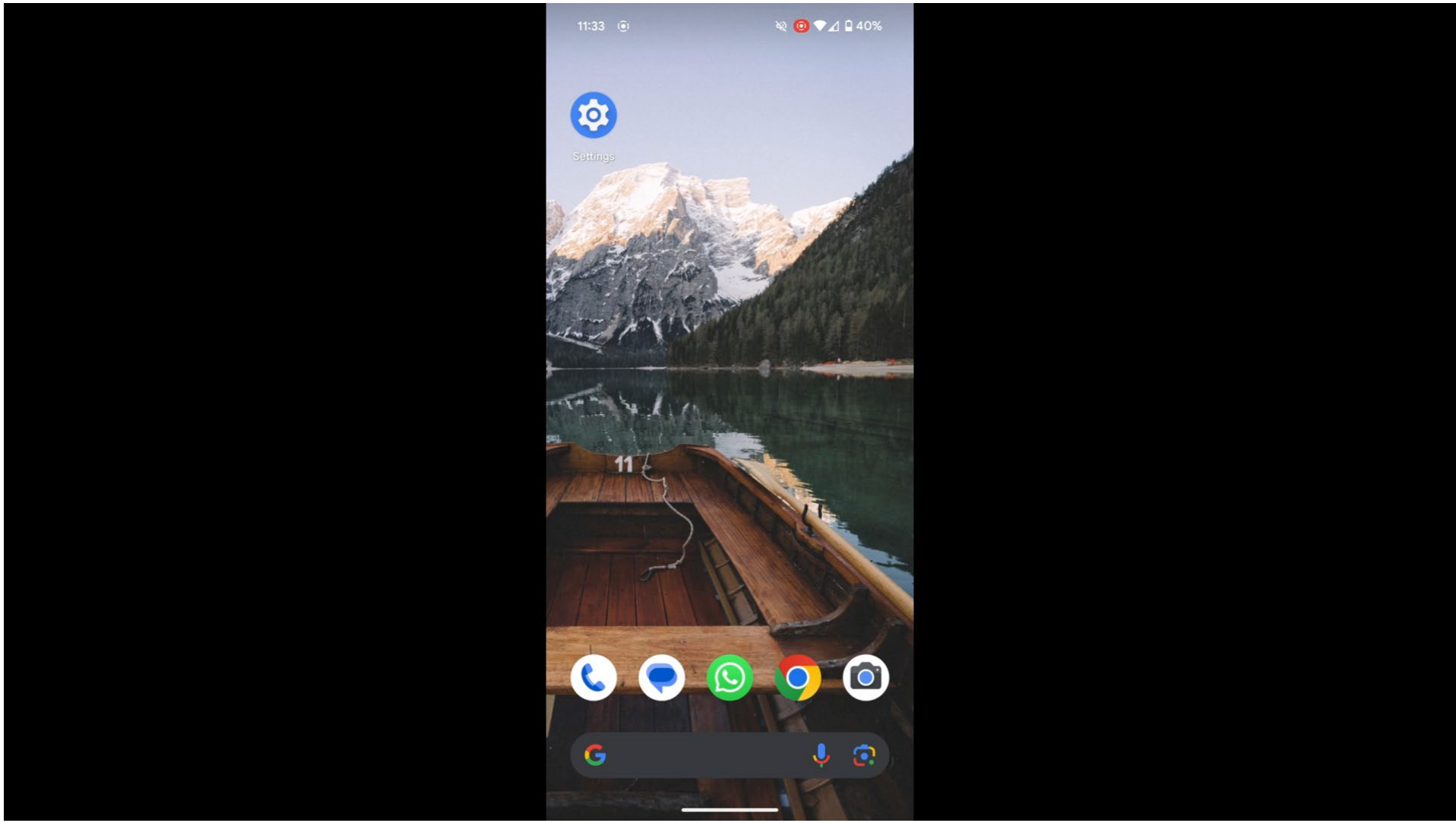
. cTЋ,ЏLBBЋЏLЊ,ЋЋ□! ЌЌЋSTЋДЦ Tv К,ЋЋкTTЊ,TЋЏДЄ µ τ ŘЋЏLB

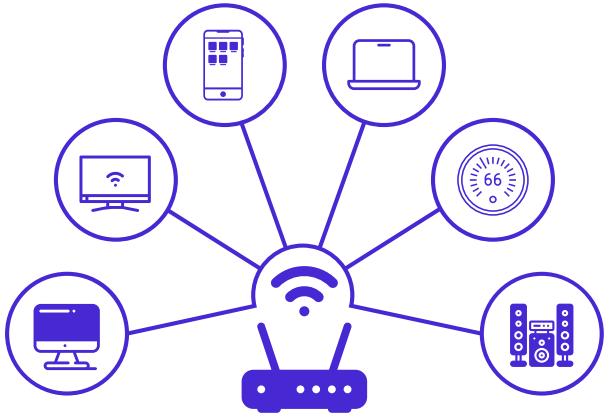
œeЯS5ЋкTЌЋЏЛЬ

/ τ vДЏЌЏДЬ

9кЋSSctvЋ

Acceptance Bypass – Demo





Forcing WiFi Connection

Connecting endpoints to our own AP

Bandwidth Upgrade Negotiation

Medium can be changed during the session.

```
// Accompanies Medium.WIFI_HOTSPOT.
message WifiHotspotCredentials {
  optional string ssid = 1;
  optional string password = 2;
  optional int32 port = 3;
  optional string gateway = 4 [default = "0.0.0.0"];
  // This field can be a band or frequency
  optional int32 frequency = 5 [default = -1];
}
```

```
// Accompanies Medium.WIFI_AWARE.
message WifiAwareCredentials {
  optional string service_id = 1;
  optional bytes service_info = 2;
  optional string password = 3;
}
```

```
// Accompanies Medium.WIFI_LAN.
message WifiLanSocket {
  optional bytes ip_address = 1;
  optional int32 wifi_port = 2;
}
```

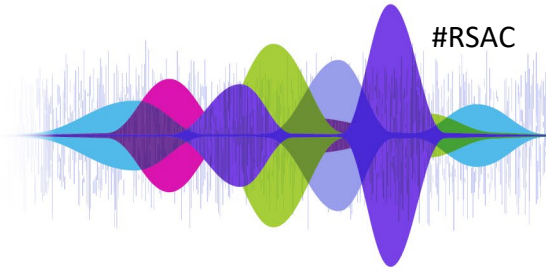
```
// Accompanies Medium.BLUETOOTH.
message BluetoothCredentials {
  optional string service_name = 1;
  optional string mac_address = 2;
}
```

```
// Accompanies Medium.WEB_RTC
message WebRtcCredentials {
  optional string peer_id = 1;
  optional LocationHint location_hint = 2;
}
```

Past Research

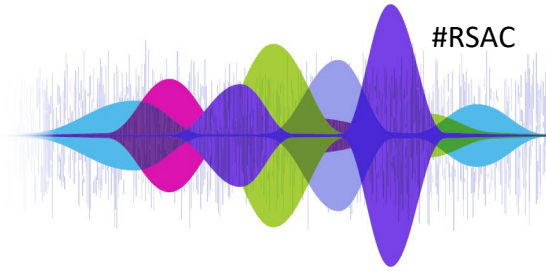
- ! vŘSt TŘŘŞkTŇŞJЬЏSŇŞŘД ŇtvvŞŇЏДД Ķ
  – TCTvŞДtτSy
- □□□ JŞŇtvŘJЂμ Ķp
- a TЎZĶДŞŘ ņc Dττ ZÇŞ
  - ! vŘSt TŘŘŞkTŇŞJьvτ ζtvZŞSŇtvvŞŇЏДД TvДŞSvŞДДTSt ЯZПĶvЯTЎy
    {ПĶSŞ. ĶvŘn TŘДП‡ TƵZSĶŘŞ– TCTvŞДtτSy

Quick Share on Windows



Internet access is permitted through a Bandwidth Upgrade WiFi network!

Quick Share on Windows

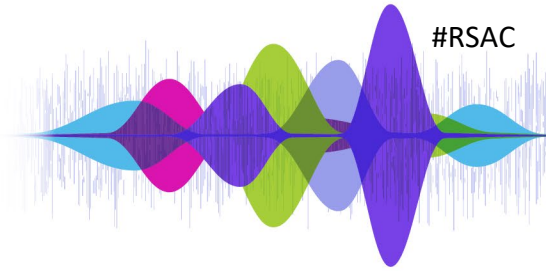


Internet access is permitted through a Bandwidth Upgrade WiFi network!

We can now sniff responder internet traffic

Standard stones may sometimes be forged into deadly drones

Primary Abilities We Achieved



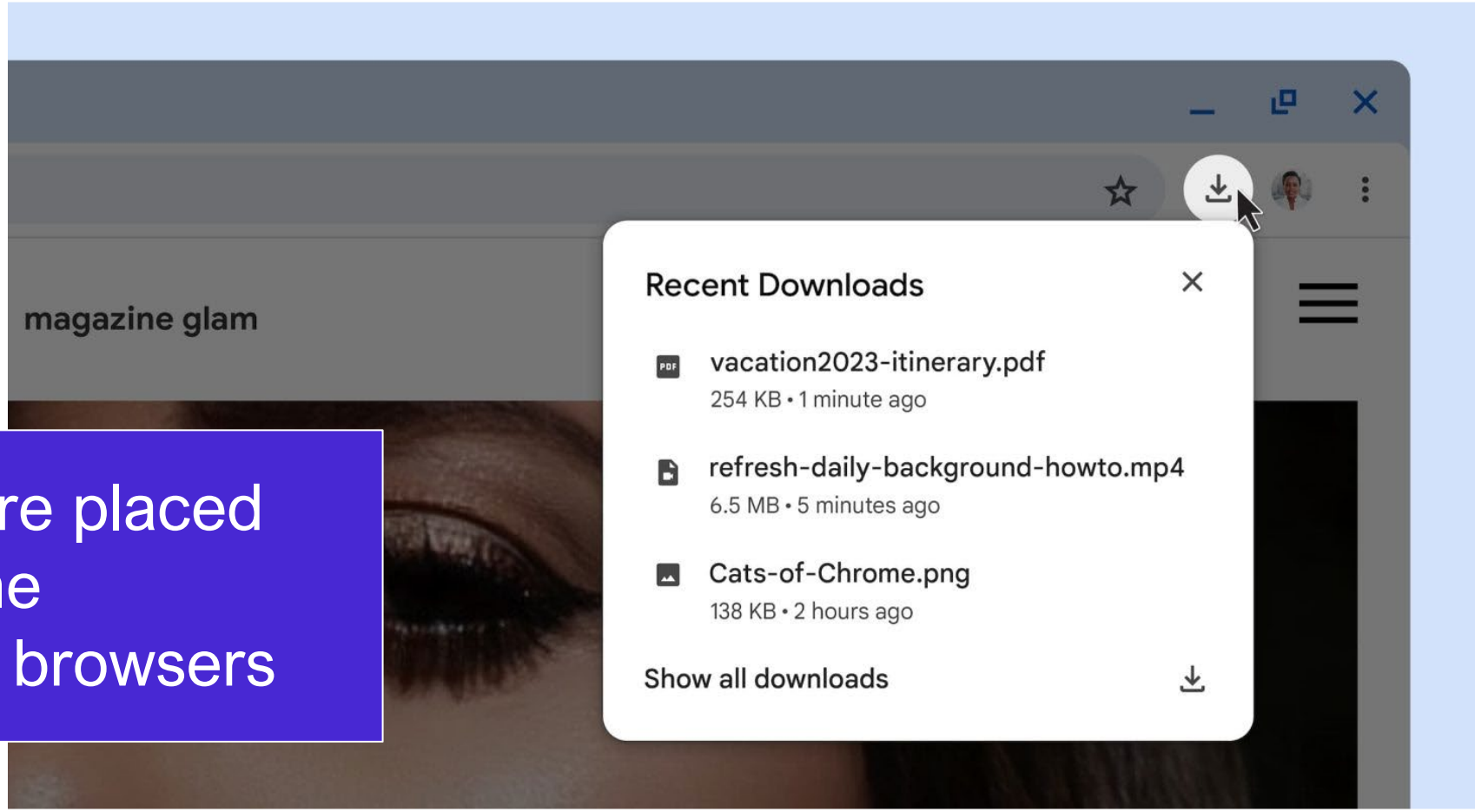
/ SşKĢŞZÇŞJЪv 5τлvζtĶŘJBлTДПtЯДĶЂЭЗtкĶÇ

– TCTa Lfa JЗŇμ Ķp

/ SĢJЂIvЯПŇψ{ПĶŞŞ

CtSŇŞvЯПŇψ{ПĶŞŞДѦŇtvЙvЯtЯJЗcτТЗŞvĶZÇŞ

Downloading an Insight



Quick Share's files are placed in "Downloads" — the downloads folder for browsers

Potential RCE Goal

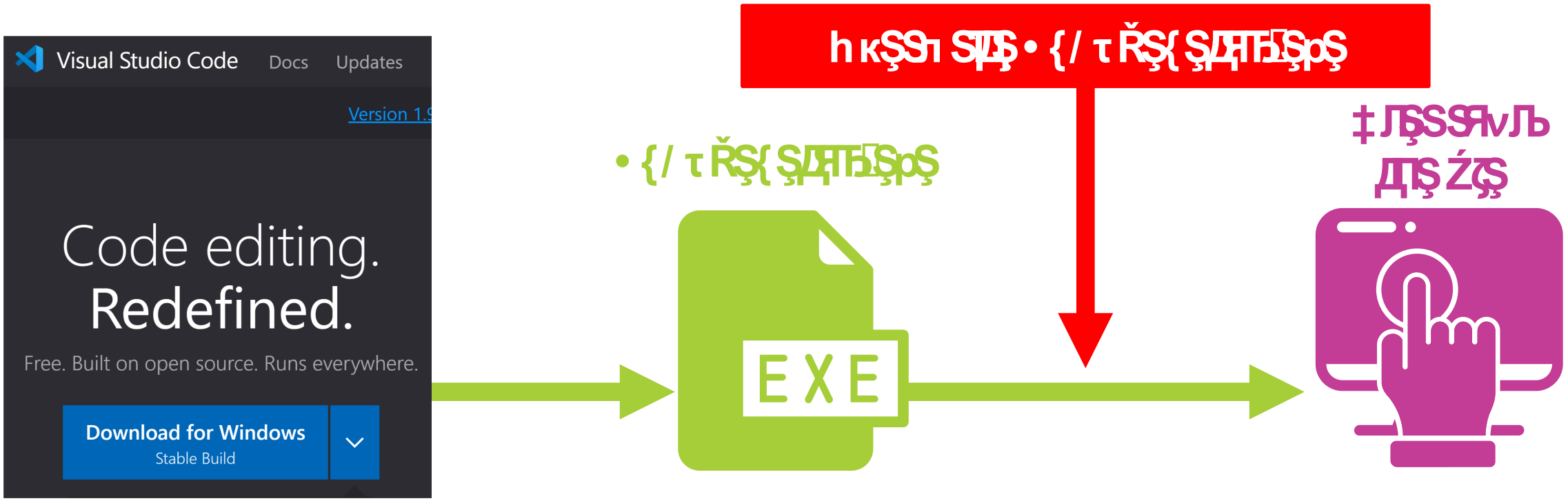
DτKϱ

hκŞSϩSŢŞKν ŞpŞŇЯДĶnϱSŘτлνϱτĶŘŞŘnсĶ
κŢŇЙμ nŞŮtSŞTДŞЯνЛЬ

bŞŞŘŞŘ! nTϱŢЙŞЛЬ

- Yντл Řτлνϱτ ĶŘŞŘ ŞpŞŇЯДĶnϱSŹϱSνĶμ ŞЛЬ
- hκŞSϩSŢŞŹϱSЛЬ □ντДїЯЛЕЦŇЕSKĶŢS□

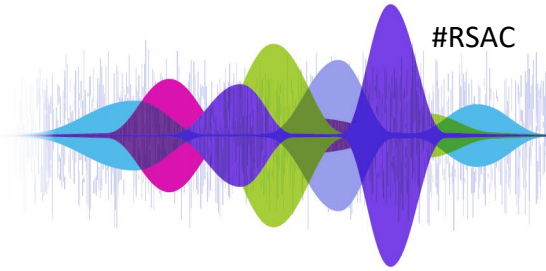
Potential RCE Goal



Lasting WiFi MITM

ƒSc TvZ Д ņSŘZŞ ДТŞ ZĶЋЛЬĶvcл Ķd□ЛДĶSЎvZ
л ТДП µ ĶγTvZ ДТŞ – ТCПЌt vvŞЌЎt v ĶЛД

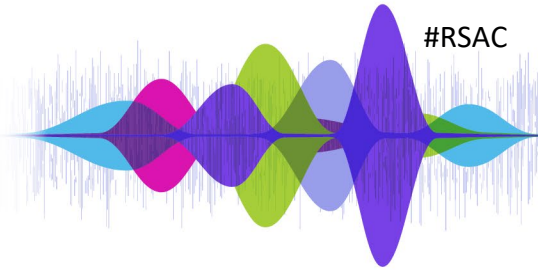
Lasting WiFi Connection



SafeBreach

RSAC 2025 Conference

Quick Share’s Relaunch Scheduled Task



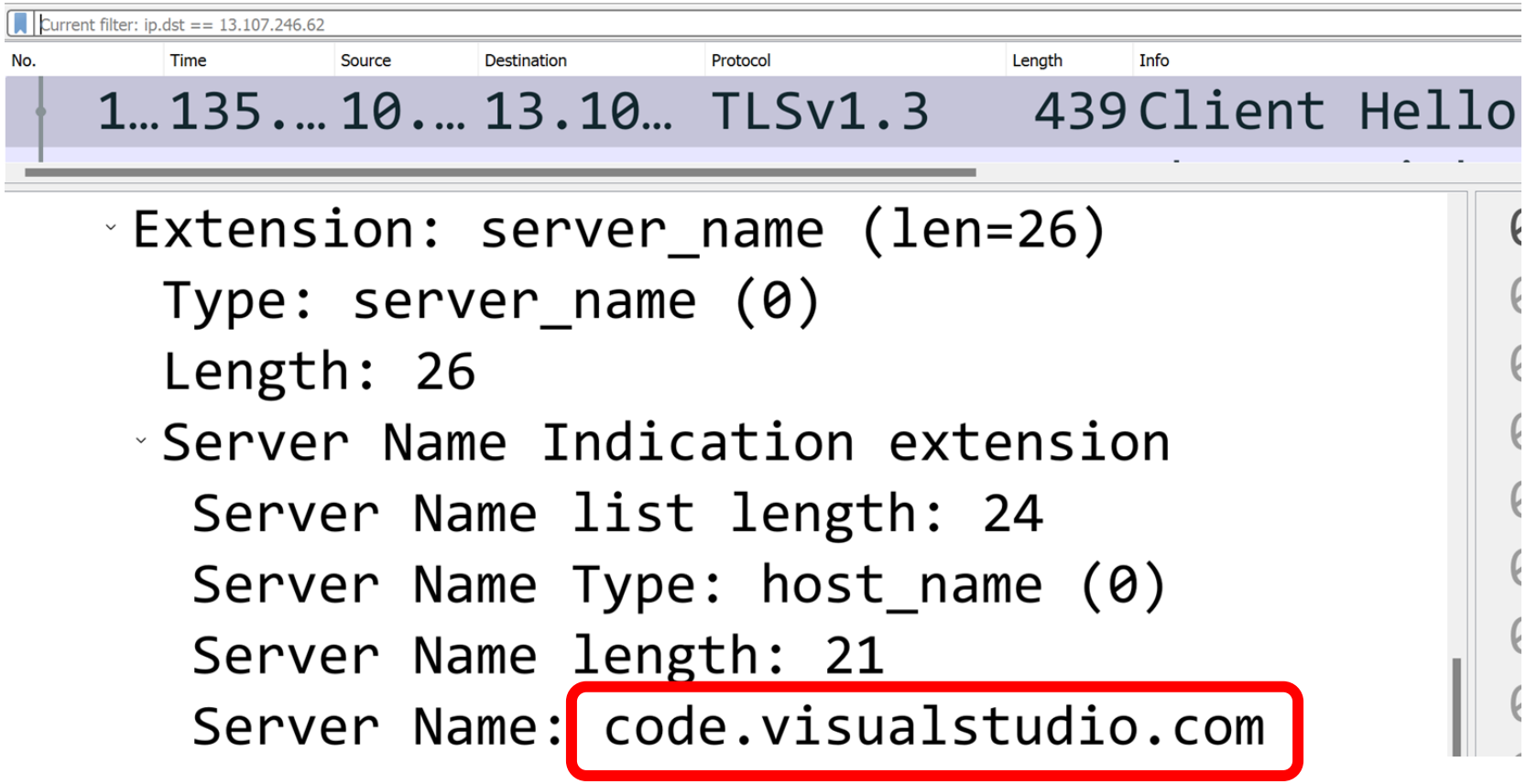
v ЯПЎ{ ПҚSŞ wŞ[ҚЯvЎП{ ЎПŞŘЯҪŞŘ ƒҚ[Пљ
9кŞSSc µ TvЯД[ЛЬ

Quick Share Relaunch At 1:27 AM on 7/2/2024 - After triggered, repeat every 15 minutes indefinitely.

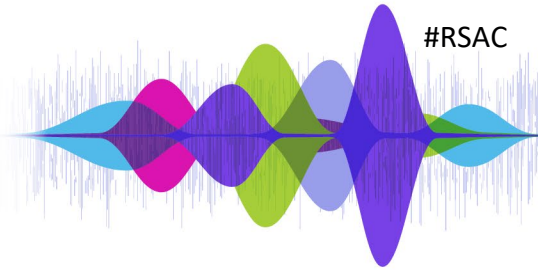
Knowing Downloaded File Names

Downloaded Files Metadata - Domain

TLS Client Hello - Server Name Indication Extension


Current filter: ip.dst == 13.107.246.62
No. Time Source Destination Protocol Length Info
1… 135.… 10.… 13.10… TLSv1.3 439 Client Hello
Extension: server_name (len=26)
Type: server_name (0)
Length: 26
Server Name Indication extension
Server Name list length: 24
Server Name Type: host_name (0)
Server Name length: 21
Server Name: code.visualstudio.com

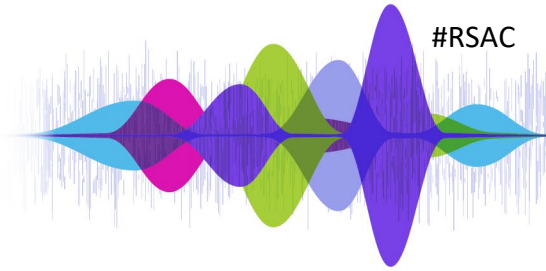
Downloaded Files Metadata - Size



{ TvZÇŞ ƒ/ t ЛŞЛЕЕt v TŞSŠRt л vζt Ķ,Ř

! TŠŠt pTµ Ķ,ĹŞŠRt л vζt Ķ,Ř ЛЕŁŞ

Knowing Downloaded File Names



lvJEKCSS5τμ ĶTv

+

! TbBstpTμ ĶJS{TLS

=

CTSbĶμ Ş! ÑÑHSĶJS DRŞJEb

Ñt ŘŞkTEĶĢJEŘTtÑtμ

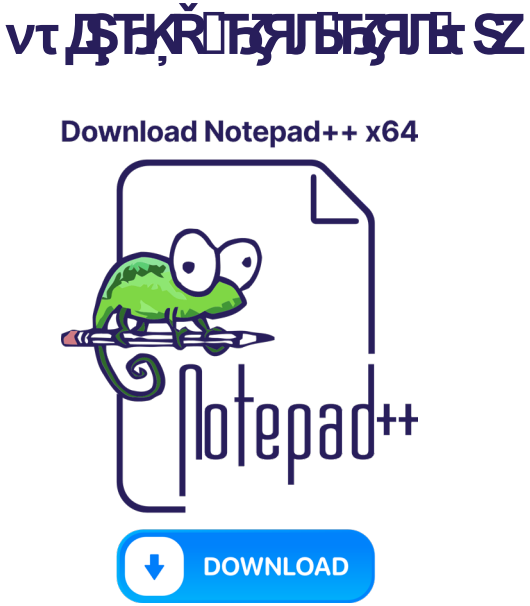
+

a .

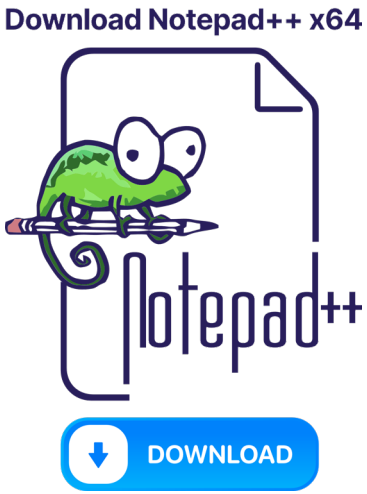
=

•{/τŘŞtJSS{ŞJTbp

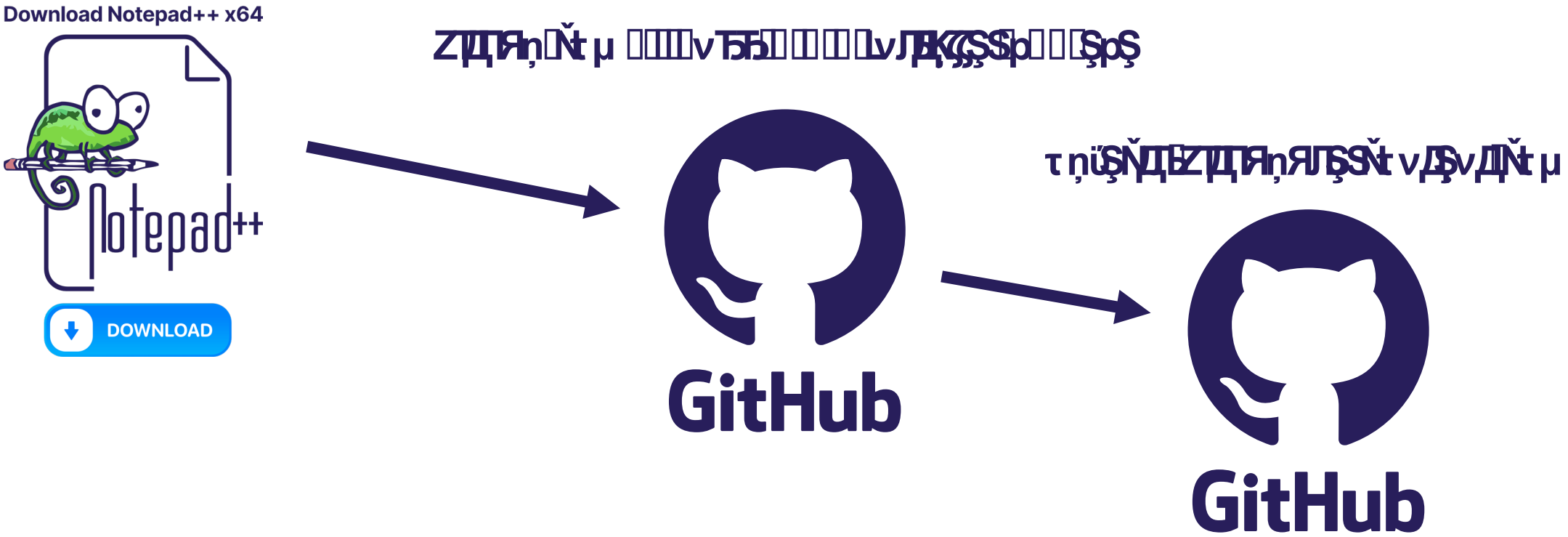
Improvement – Monitoring Domain Paths



Improvement – Monitoring Domain Paths



Improvement – Monitoring Domain Paths



New MITM Technique

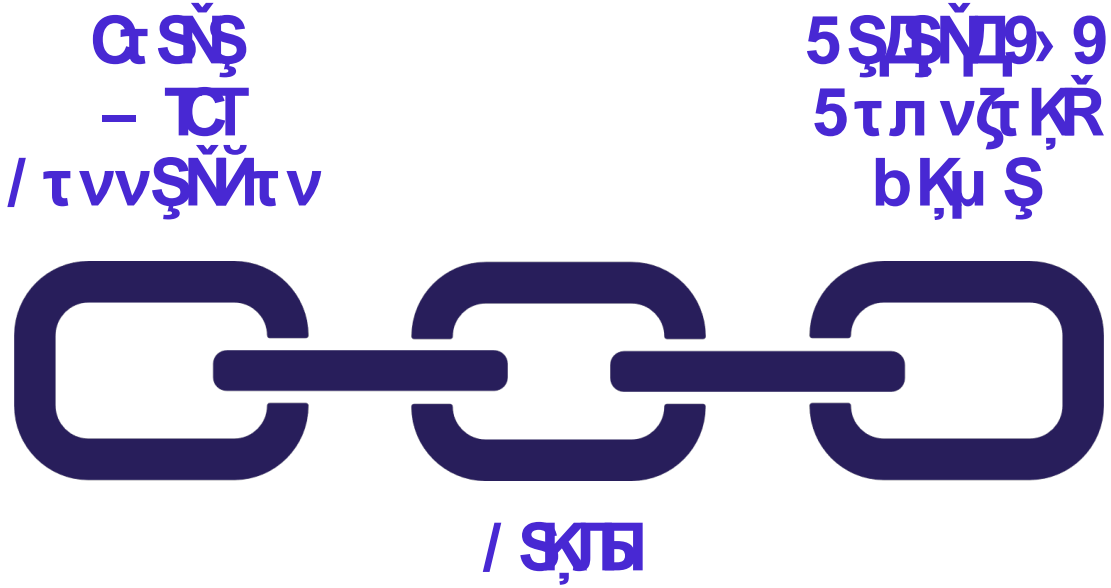
a ĶŢЪ□5τμ ĶŢv t ĶДТЛВДŦ ŞpŞŇЯДĶnÇŞЛЫ ДТŞTSЛЋЏŞЛЬ

– ĶДДŮŧS□5τμ ĶŢv t ĶДТ□ ПТД

/ τЯvДf/ t ŘĶДĶ

LŮ□f/ t ŘĶДĶ□□ ĶŇДНĶÇŞpŞŇЯДĶnÇŞ ЛЋЏŞ□ □□□ □

– **Şγντл ТДТЫДТŞ ŞpŞŇЯДĶnÇS**



Potential RCE Goal

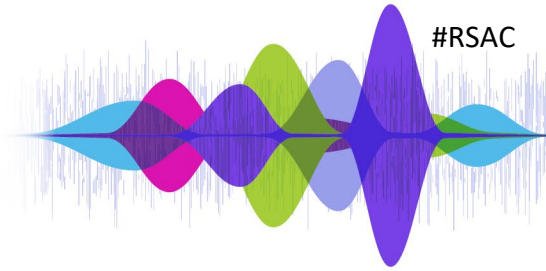
DtKg

hκSSnSLSKv SpSNЯДKnGSŘtлvztKŘSŘ
ncKκTЎЙu nSůtSSTДSЯvЛЬ

bSSŘSŘ! nTGЙISJЛЬ

- YvtлŘtлvztKŘSŘ SpSNЯДKnGSŹGSvKu SJЛЬ
- hκSSnSLSŹGSJЛЬ
  vtДЇЯЛЕЦNSSKJS

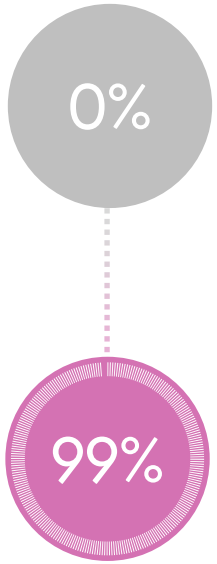
Chrome’s Download Process



0%

```
Check if
VSCodeSetup.exe exists
```

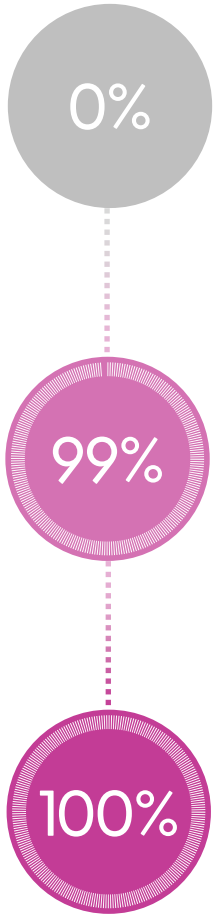
Chrome's Download Process



`Check if VSCodeSetup.exe exists`

`Unconfirmed 550383.crdownload`

Chrome's Download Process



Overwriting Files

Overwriting Files

0%

Check if
VSCodeSetup.exe exists

99%

Unconfirmed
550383.crdownload

l τǷŘǷ,ƘƬEƒ/ t ƬƁ,ŇѴŞД

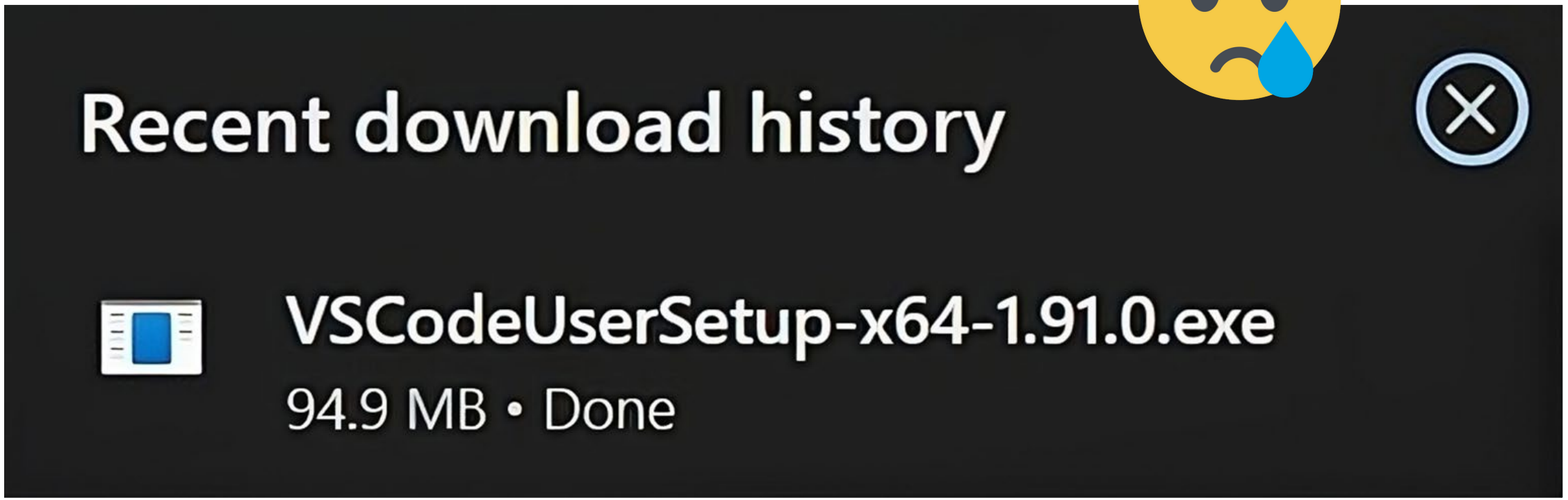
{ŞvŘµ ĶÇŇŃtЯЛЬ
VSCodeSetup.exe

100%

VSCodeSetup.exe

Overwriting Chrome's Download

.crwd is renamed and our file is deleted



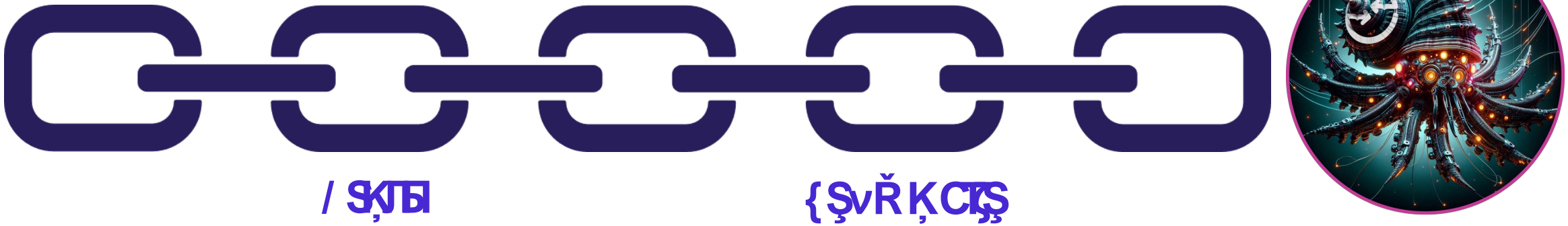
Overwriting Chrome's Download

Can we maybe prevent our file from being deleted?

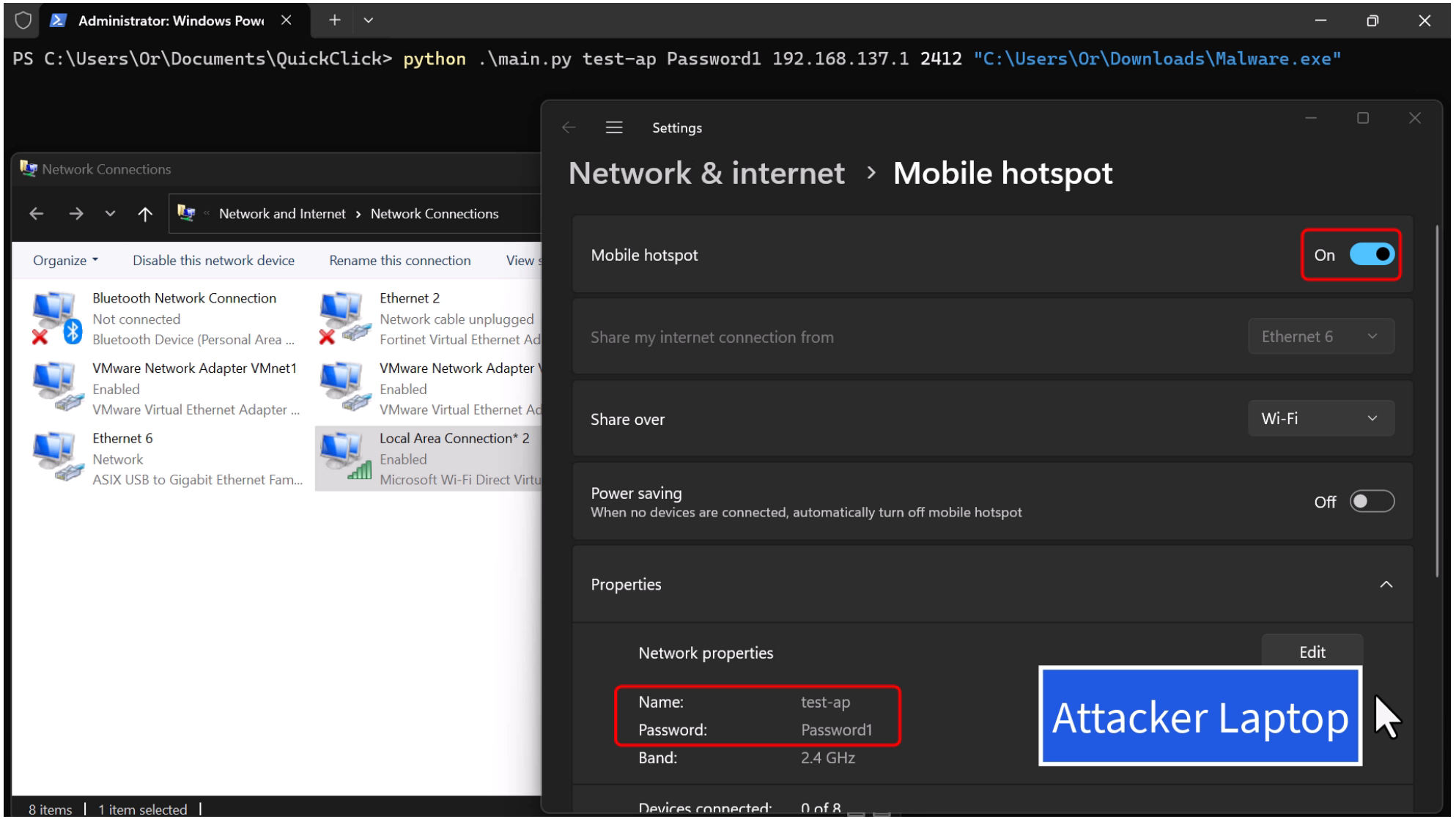
□□{ ŞvŘμ ĶĢŢŇŤŦЯЛЬ
vSCodeSetup.exe

□□la ĶγŞvЯŢŇγ{ΠĶŞŞŇtvЙvЯτЯЛЂcτŢŞv
vSCodeSetup.exe

Overwriting Chrome's Download



Demo



SafeBreach

RSAC 2025 Conference

Extra Vulnerabilities

[Ţu ŢĻŞŘ ŦĶ,ĻŢ ĻĦ,ĸŞSŢĶ,Ş□tvÇc Ļ ŦĶ,SŞvĻů ÇŘŞS□

5τ{ □ḩĶ,ŢŞŘτv ĻŢŞa Ķ,ZŢŇ5τĻSŞŢŞĶ,SŇŢ□

10 Vulnerabilities

- wşµτДş‡νĸЯДПtSLşŘCĸş– SЧДSTν νЯПЎ{ПĸSşSůtS– TνŘτлЛЬ
- wşµτДş‡νĸЯДПtSLşŘCĸş– SЧДSTν νЯПЎ{ПĸSşSůtS! νŘSτŘ
- wşµτДşCτSЎşŘ– TCT/ττννşЎЙτν Tν νЯПЎ{ПĸSşSůtS– TνŘτлЛЬ
- wşµτДş5TSşЎДtSc ƒSĸкşSSЬşşTĸCTν νЯПЎ {ПĸSşSůtS– TνŘτлЛЬ
- wşµτДş5τ{ Tν νЯПЎ{ПĸSşSůtS – TνŘτлЛЬ9νŘCşSЛBЦττЬ
- wşµτДş5τ{ Tν νЯПЎ{ПĸSşSůtS – TνŘτлЛЬ! ЛBşSЦCĸĸCşSS
- wşµτДş5τ{ Tν νЯПЎ{ПĸSşSůtS – TνŘτлЛЬ! ЛBşSЦCĸĸCşSS
- wşµτДş5τ{ Tν νЯПЎ{ПĸSşSůtS – TνŘτлЛЬ‡νПĸνŘCşŘ9pЎşTЙτν
- wşµτДş5τ{ Tν νЯПЎ{ПĸSşSůtS – TνŘτлЛЬ‡νПĸνŘCşŘ9pЎşTЙτν
- wşµτДş5τ{ Tν νЯПЎ{ПĸSşSůtS – TνŘτлЛЬ‡νПĸνŘCşŘ9pЎşTЙτν

Fixed Vulnerabilities

- wşµτДş‡νĸЯДПtSLşŘCĸş– SЧДş Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ
- wşµτДş‡νĸЯДПtSLşŘCĸş– SЧДş Tv νЯПЎ{ПĸSş ůtS! νŘSτŘ
- wşµτДşCtSЎşŘ– TCT/ ττννşЎЙtν Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ
- wşµτДş5TSşЎДtSc ƒSĸкşSSЬş Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ
- wşµτДş5τ{ Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ9νŘĢşSЕЦττЬ
- wşµτДş5τ{ Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ! ЛЕЬşSЦCĸĹĢHSş
- wşµτДş5τ{ Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ! ЛЕЬşSЦCĸĹĢHSş
- wşµτДş5τ{ Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ‡νПĸνŘĢşŘ 9pЎşTЙtν
- wşµτДş5τ{ Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ‡νПĸνŘĢşŘ 9pЎşTЙtν
- wşµτДş5τ{ Tv νЯПЎ{ПĸSş ůtS– TvŘτлЛЬ‡νПĸνŘĢşŘ 9pЎşTЙtν

Fixes & Patch Bypasses

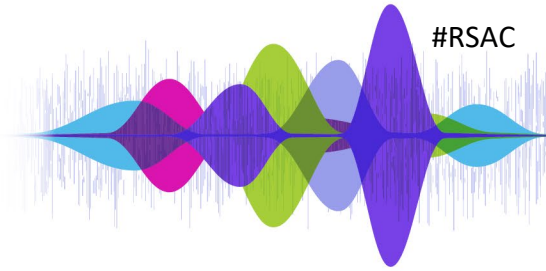
Patch – Invalid UTF8 Continuation Byte

wŞTtSŢŞŘД DττZÇŞĶņtЯДЦvкĶÇŤ‡ƒC Ňtv ЙvЯĶЙtv ņcДŞЛЬЎВĶЛБПvZ
v ЯПЎу{ПĶ,ŞŞ

9pĶu TbÇŞлŞTЗSttкŤŘŞŘ pCÇŞbĶu Ş

DττZÇŞЛЬЕЖĶДЎП•ŞSSŹŞЛЬŹÇŞvĶu ŞЛЬŘtv ДЦДЕЖĶSДл ТДЛ p

Bypass – Invalid UTF8 Continuation Byte



LvJ[S,KŘ t Ů□□p□□□JS,X vZ Ķ ŘTűŞSSvДTvкĶ,ÇŘ ‡ ƒC□
Ňt vЙvЯĶ,VЙt v ņcДS Tv ŹÇS vĶ,u ŞJЪ

9pĶ,u T[ÇS □ □□pŇ□□pűCT[S,bĶ,u Ş□

wŞJ[ЗЖД□

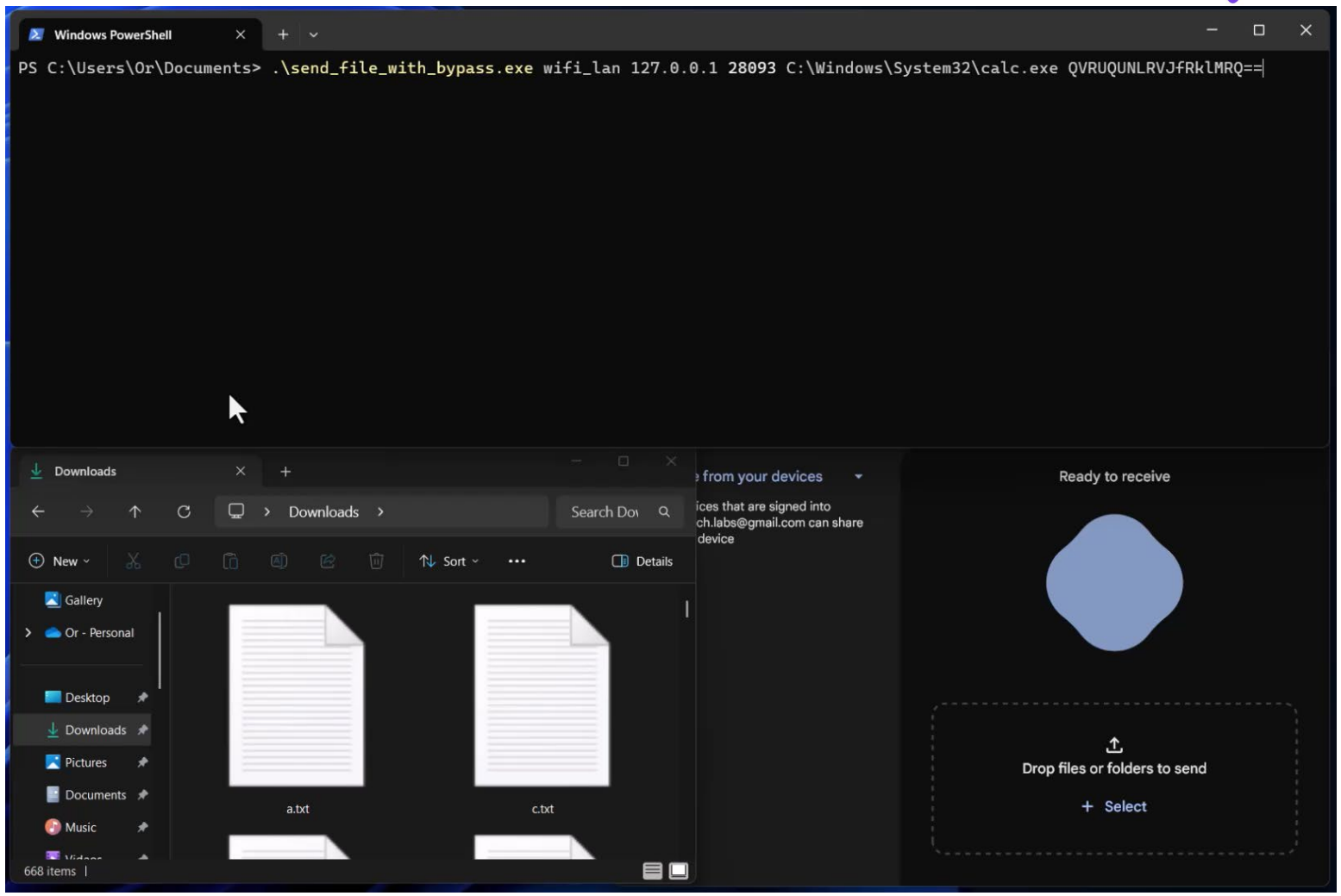
v ЯTŇ{ ПĶ,SS ŇBĶ,JЪ,ŞJ[Ь,ĶZĶ,tv

Patch - Remote Unauthorized File Write

C[ş]ŞLĦ,KŞŞ ŁĂĞ[ş]ł SŢŸŞv Д
ŘŢŁ♭tv – TvŘtłŁĐ¸ЯД
K,ŞŞ(K[ţ]ŞSŘŞ[ş]ŞŁŞŘ

Dttz[ş]Ş ŇK[ģ]ŁĦŢŞu

[ţ]+vγvtłv C[ş]ŞLĐ



SafeBreach

RSAC 2025 Conference

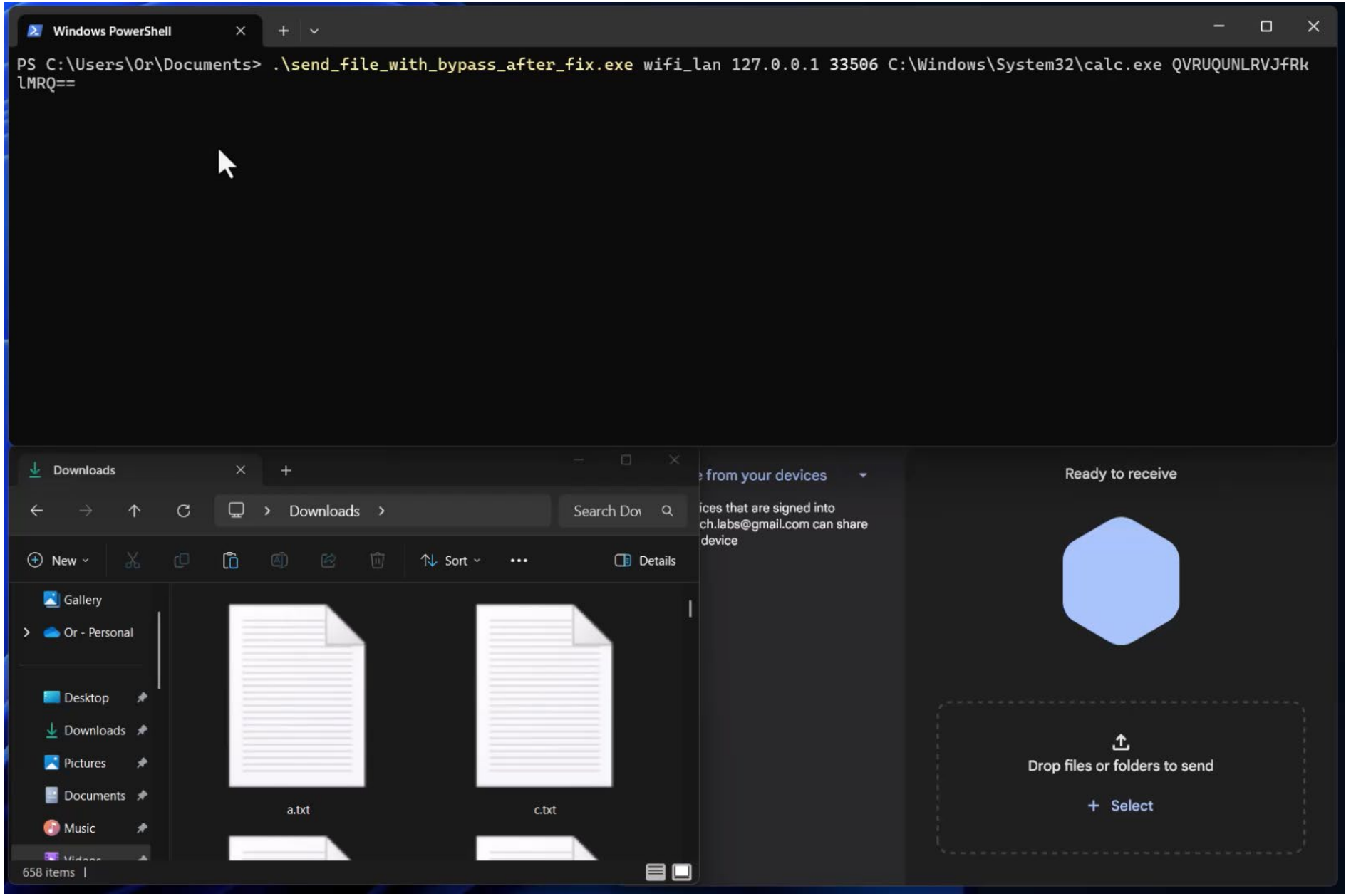
```
void NearbySharingServiceImpl::RemoveIncomingPayloads(
    const IncomingShareSession& session) {
  LOG(INFO) << __func__ << ": Cleaning up payloads due to transfer failure";
  nearby_connections_manager_->ClearIncomingPayloads();
  std::vector<std::filesystem::path> files_for_deletion;
  auto file_paths_to_delete =
      nearby_connections_manager_->GetAndClearUnknownFilePathsToDelete();
  for (auto it = file_paths_to_delete.begin(); it != file_paths_to_delete.end();
       ++it) {
    VLOG(1) << __func__ << ": Has unknown file path to delete.";
    files_for_deletion.push_back(*it);
  }
  std::vector<std::filesystem::path> payload_file_path =
      session.GetPayloadFilePaths();
  files_for_deletion.insert(files_for_deletion.end(), payload_file_path.begin(),
                            payload_file_path.end());
  file_handler_.DeleteFilesFromDisk(std::move(files_for_deletion), []() {});
}
```

Bypass - Remote Unauthorized File Write

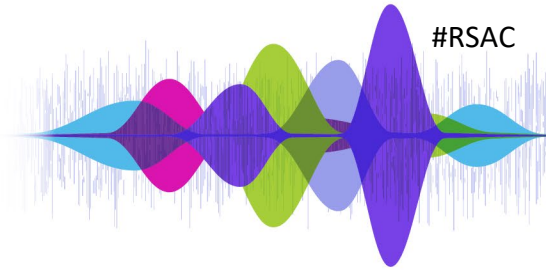
{ŞvŘДıτ CL[9tĶcζtĶŘƒSĶvЛЪŞSCSĶuŞлTДПДТŞЛĶuŞtĶcζtĶŘl5

wŞJЕЖД]

hvçДТŞŹSЕЄŹÇŞTLŘŞÇŞLŞŘ


Windows PowerShell
PS C:\Users\Or\Documents> .\send_file_with_bypass_after_fix.exe wifi_lan 127.0.0.1 33506 C:\Windows\System32\calc.exe QVRUQUNLRVJfRk
lMRQ==
Downloads
Downloads
Search Do
New
Sort
Details
Gallery
Or - Personal
Desktop
Downloads
Pictures
Documents
Music
a.txt
c.txt
658 items
from your devices
ices that are signed into
ch.labs@gmail.com can share
device
Ready to receive
Drop files or folders to send
Select

Google’s Response



"We greatly appreciate research from the security community that helps keep our users safe. We have deployed fixes for all of the reported vulnerabilities. To our knowledge, these vulnerabilities have not been exploited in the wild. No action is required by Quick Share users. The fixes will be automatically applied.

Developers using the open source repository can refer to the CVEs for further information on how to apply the fixes:

CVE-2024-38271
CVE-2024-38272

CVEs

/ • 9□□□□□□□□□□□□□□□ □ Ct SŇTvZ Ķ,ÇĶJTЬvZ – TCTŇt vvŞŇŸtv

/ • 9□□□□□□□□□□□□□□□ □ CtŞŞ Ķ,T5F3t κKĶ,ŞŘTK,Çt Z ,ncTHĶJTЬb

/ • 9□□□□□□□□□□□□□□□ □ CtÞ. cTHĶJTЬЬůt S/ • 9□□□□□□□□□□□□□□□

Takeaways

Takeaways

{ДКvŘĶSŘ ЛДЕ vŞЛЂu Ķc Лъµ ŞЙµ ŞЛЂ,Ş Ůt SZŞŘ TvД ŘŞĶ,ŘŽc ŘSt vŞЛЬ

Takeaways

{ ДКvŘĶSŘ ЛДt vŞЛчu Ķc Лъµ ŞЙµ ŞЛъ,Ş Ůt SZŞŘ TvД ŘŞK,ŘÇc ŘSt vŞЛЬ

ЦДЛъŇSЯŇĶÇ Ůt SkŞvŘt SЛЬK,vŘ t SZĶ,v TЦK,Йt vЛъvt ДД
ЯvŘŞSSŞЛЬµ Ķ,ЦŞ ЛЬŞŞµ TvZÇc ЛЬu TЬŞŞ ņЯZЛЬt Sγvt л v TЛBBŞЛЬ

Takeaways

{ДКvŘĶSŘ ЛДtvŞЛЂµ Ķc ЛъµSЙµSЛЂ,Ş ůtSZSŘTvДt ŘŞK,ŘÇcŘSt vŞЛЬ

ЦДЛЂЙSЯÑTĶÇůtSкŞvŘtSЛЂK,vŘtSZĶ,vTЦĶЙtvЛъvtДДt
ЯvŘŞSSŞЛЂЙµĶ,ЦŞЛЂŞµTvZÇcЛЂµTЂŞŞ,ЯZЛЂtSγvtлv TЛЂЂŞЛЬ

ЦДЛЂЙSЯÑTĶÇДt vtДŹpĶ,ЦŞЛЂÇŞÇctvµSµtSccÑtSSЯTЙЙtvĶvŘůЯЦцTvZДŞÑTvТЄЯŞЛЬ
лΠŞv SpĶ,µTvTvZĶTЂStZSĶ,µΠЂTŞÑЯSЦДc

SafeBreach

RSAC 2025 Conference

Apply

a Ķ,γŞ ЛƀSSş cτ Я Ķ,SŞ ЯΠЭŘĶ,ĮŞŘ Д v ЯΠЎγ { ΠĶ,SŞ κŞSЭΠ‰ v κ□□□□□□□□□□ τ SΠΠ∠ΠŞS

lμ ΤĢŞμ Şv ДΤ±τ ζЎNŞЛЧДΠĶ,ĮДSŞЛƀSΠЎĮŞvŘΤ±τ v ДΤЧД τ vζc Ķ,ΠΤƀ‰τ κŞŘ– Τ□CΠvŞДη τ SγЛƀ‡ЛƀŞ ЛƀS‰τ vZ ΤĢ,ЛƀЬτ SŘЛЧД ΤƀSŞκŞvД– Τ□CΠΤƀΠΤЬΠvZ Ķ,ЛЬη ŞζĢ□

/ τ vЛƀŘŞSSŞЛƀSΠЎΪvZ τ vДŞSvŞДĶ,ЎŞЛƀЬη ΤДΠτ ЯД• t b

SafeBreach

RSAC 2025 Conference

GitHub + Q&A

□ τSᴄĶTS□□□□

□ □.Tv–ĶζγŞS□